BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

SP

OFICINA ESPAÑOLA

ES99/115

de

PATENTES y MARCAS

CERTIFICADO OFICIAL

Por la presente certifico que los documentos adjuntos son copia exacta de la solicitud de PATENTE de INVENCION número 9801037, presentada en este Organismo, con fecha 7 de Mayo de 1998.

Madrid, 3 de junio de 1999

El Director del Departamento de Patentes
e Información Tecnológica.

P.D.

M. MADRUGA

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

OFICINA ESPAÑOLA DE PATENTES Y MARCAS

INSTANCIA DE SOLICITUD DE:

☒ PATENTE DE INVENCION ☐ MODELO DE UTILIDAD

NUMERO DE SOLICITUD
P9801037

FECHA Y HORA DE PRESENTACION EN O.E.P.M.
11 h. 36 mn 07 MAIG 1998

FECHA Y HORA DE PRESENTACION EN LUGAR DISTINTO O.E.P.M.

(1)
☐ SOLICITUD DE ADICION
☐ SOLICITUD DIVISIONAL
☐ CAMBIO DE MODALIDAD
☐ TRANSFORMACION SOLICITUD EUROPEA

(2) EXPED. PRINCIPAL O DE ORIGEN
MODALIDAD
NUMERO SOLICITUD
FECHA SOLICITUD
MODALIDAD
NUMERO SOLICITUD
FECHA SOLICITUD

(3) LUGAR DE PRESENTACION: BARCELONA — CODIGO: 08

(4) SOLICITANTE(S)	APELLIDOS O DENOMINACION JURIDICA	NOMBRE	DNI
	FERRE HERRERO	ANGEL JOSE	40923966

OFICINA ESPAÑOLA DE PATENTES Y MARCAS
Dpto. SECRETARIA GENERAL
REPROGRAFIA
Panamá, 1 - Madrid 28071

(5) DATOS DEL PRIMER SOLICITANTE

DOMICILIO: AVGDA. CONSTITUCIO, 3 BIS, 3º
LOCALIDAD: SANT CARLES DE LA RAPITA
PROVINCIA: TARRAGONA
PAIS RESIDENCIA: ESPAÑA
NACIONALIDAD: ESPAÑOLA
TELEFONO: 977740661
CODIGO POSTAL: 43540
CODIGO PAIS: ES
CODIGO NACION: ES

(6) INVENTOR(ES)

(7) ☒ EL SOLICITANTE ES EL INVENTOR
☐ EL SOLICITANTE NO ES EL INVENTOR O UNICO INVENTOR

(8) MODO DE OBTENCION DEL DERECHO
☐ INVENC. LABORAL ☐ CONTRATO ☐ SUCESION

APELLIDOS	NOMBRE	NACIONALIDAD	COD. NACION
FERRE HERRERO	ANGEL JOSE	ESPAÑOLA	ES

(9) TITULO DE LA INVENCION

DISPOSITIVO DE ALEATORIZACION-ENCRIPTACION DE SECUENCIA DE DATOS

(10) INVENCION REFERENTE A PROCEDIMIENTO MICROBIOLOGICO SEGUN ART. 25.2 L.P. ☐ SI ☒ NO

(11) EXPOSICIONES OFICIALES

LUGAR ..... FECHA .....

(12) DECLARACIONES DE PRIORIDAD

PAIS DE ORIGEN	COD. PAIS	NUMERO	FECHA

(13) EL SOLICITANTE SE ACOGE A LA EXENCION DE PAGO DE TASAS PREVISTA EN EL ART. 162 L.P. ☐ SI ☒ NO

(14) REPRESENTANTE — APELLIDOS — NOMBRE — CODIGO

DOMICILIO — LOCALIDAD — PROVINCIA — COD. POSTAL

(15) RELACION DE DOCUMENTOS QUE SE ACOMPAÑAN

☒ DESCRIPCION. N.º DE PAGINAS... 33
☒ REIVINDICACIONES. N.º DE PAGINAS... 5
☒ DIBUJOS. N.º DE PAGINAS... 9
☒ RESUMEN
☐ DOCUMENTO DE PRIORIDAD
☐ TRADUCCION DEL DOCUMENTO DE PRIORIDAD
☐ DOCUMENTO DE REPRESENTACION
☐ PRUEBAS
☒ JUSTIFICANTE DEL PAGO DE TASAS
☐ HOJA DE INFORMACIONES COMPLEMENTARIAS
☐ OTROS

FIRMA DEL FUNCIONARIO

FIRMA DEL SOLICITANTE O REPRESENTANTE

(16) NOTIFICACION DE PAGO DE LA TASA DE CONCESION

Se le notifica que esta solicitud se considerará retirada si no procede al pago de la tasa de concesión; para el pago de esta tasa dispone de tres meses a contar desde la publicación del anuncio de la concesión en el BOPI, más los diez días que establece el art. 81 del R.D. 10-10-86.

1. O.E.P.M. Expediente

ILMO. SR. DIRECTOR DE LA OFICINA ESPAÑOLA DE PATENTES Y MARCAS

UNE A-4 MOD. 3101

CUMPLIMENTAR LOS TRES EJEMPLARES SALVO ZONAS EN ROJO

PATENTE
RESUMEN Y GRAFICO

NUMERO DE SOLICITUD
P 9 8 0 1 0 3 7

FECHA DE PRESENTACION

RESUMEN (Máx. 150 palabras)

Dispositivo de aleatorización-encriptación de secuencia de datos tal que suministradas secuencia de datos de entrada (X) y clave de aleatorización-encriptación (Kp), genera secuencia de datos aleatoria (Yp), tal que no expertos en encriptación pueden medir objetivamente la confusión y difusión de la secuencia generada (Yp) por la clave de aleatorización-encriptación utilizada (Kp).

Dicho dispositivo hace uso del dispositivo objeto de la patente estadounidense número 5,214,703 de título "Device for the conversion of a digital block and use of same" para lograr sus propósitos. La secuencia de datos (X) es dividida en bloques (XI), cada bloque (XI) se agrupa con bloque de control (WI), el bloque resultado de la agrupación (VI) es encriptado con el mencionado dispositivo objeto de la patente estadounidense número 5,214,703 (204) dando como resultado un bloque de salida (YI), el cual se suministra como nuevo bloque de control (WI) y a su vez también forma parte de la secuencia aleatorizada-encriptada (Yp) de salida.

GRAFICO

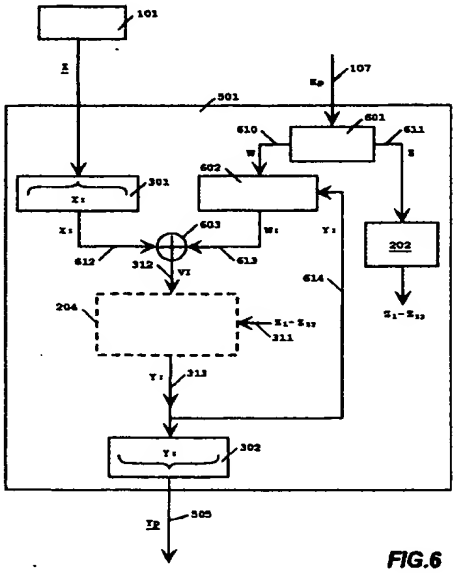

FIG.6

RESUMEN DE LA INVENCION Y GRAFICO

El resumen al que se refiere el artículo 27 de la Ley tendrá una extensión máxima de 150 palabras, deberá indicar el título de la invención y contener una exposición concisa del contenido de la descripción y reivindicaciones y, en su caso, dibujo o dibujos más característicos que deberán situarse debajo del texto del resumen.

El resumen deberá permitir una fácil comprensión del problema técnico planteado, la solución aportada y el uso o usos principales de la invención.

Los márgenes mínimos serán los siguientes:

Margen superior: 2 cm.
izquierdo: 2,5 cm.
derecho: 2 cm.
inferior: 2 cm.

Las dimensiones máximas del (de los) gráfico(s) serán 8 × 8 cm.

ESPAÑOLA DE PATENTES
OFICINA Y MARCAS

DATOS DE PRIORIDAD
(31) NUMERO (32) FECHA (33) PAIS

A1 (12) PATENTE DE INVENCION
(21) NUMERO DE SOLICITUD
P 9801037
(22) FECHA DE PRESENTACION

(71) SOLICITANTE(S)
Don Angel José FERRE HERRERO

NACIONALIDAD
ESPAÑOLA

DOMICILIO
SANT CARLES DE LA RAPITA, TARRAGONA, Avgda Constitució, 3bis 3°

(72) INVENTOR(ES)
El solicitante

(73) TITULAR(ES)

(11) N.º DE PUBLICACION

(45) FECHA DE PUBLICACION

(62) PATENTE DE LA QUE ES DIVISIONARIA

(51) Int. Cl.

GRAFICO (SOLO PARA INTERPRETAR RESUMEN)

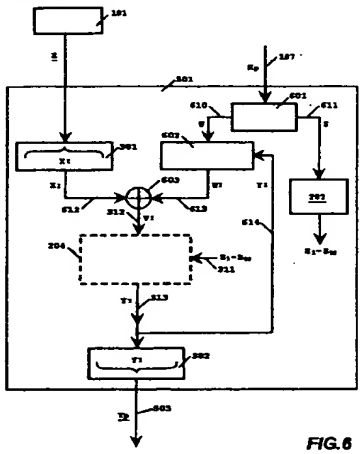

FIG.6

(54) TITULO

DISPOSITIVO DE ALEATORIZACION-ENCRIPTACION DE SECUENCIA DE DATOS

(57) RESUMEN (APORTACION VOLUNTARIA. SIN VALOR JURIDICO)

Dispositivo de aleatorización-encriptación de secuencia de datos tal que suministradas secuencia de datos de entrada (X) y clave de aleatorización-encriptación (Kp), genera secuencia de datos aleatoria (Yp), tal que no expertos en encriptación pueden medir objetivamente la confusión y difusión de la secuencia generada (Yp) por la clave de aleatorización-encriptación utilizada (Kp).

Dicho dispositivo hace uso del dispositivo objeto de la patente estadounidense número 5,214,703 de título "Device for the conversion of a digital block and use of same" para lograr sus propósitos. La secuencia de datos (X) es dividida en bloques (XI), cada bloque (XI) se agrupa con bloque de control (WI), el bloque resultado de la agrupación (VI) es encriptado con el mencionado dispositivo objeto de la patente estadounidense número 5,214,703 (204) dando como resultado un bloque de salida (YI), el cual se suministra como nuevo bloque de control (WI) y a su vez también forma parte de la secuencia aleatorizada-encriptada (Yp) de salida.

DESCRIPCION

DISPOSITIVO DE ALEATORIZACION-ENCRIPTACION DE SECUENCIA DE DATOS

La presente invención según se expresa en el título de la memoria descriptiva, se refiere a un dispositivo de aleatorización-encriptación de secuencia de datos digitales con una clave seleccionable libremente, en que la secuencia de datos encriptados de salida es substancialmente aleatoria, así como el dispositivo recuperador de la mencionada secuencia de datos digitales a partir de la secuencia aleatorizada-encriptada haciendo uso de la clave seleccionable con la cual se ha aleatorizado-encriptado.

La presente invención es especialmente aplicable en comunicaciones secretas, mantenimiento de la confidencialidad de la información, transacciones de comercio electrónico, comunicaciones por correo electrónico y semejantes.

ESTADO DE LA TECNICA

Como es conocido en el arte de la criptología, técnicas de encriptación (codificación) son usadas de modo que datos que están sujetos a vistas indeseadas, acostumbran a ser encriptados de tal forma que es difícil para uno que no esté autorizado a verlos, o usarlos, el que sea capaz de hacerlo.

Como se acostumbra en el arte de la encriptación, el término "texto claro" se refiere a texto que no ha sido codificado o encriptado y acostumbra a ser directamente legible, y el término "texto cifrado" o "texto encriptado" se utiliza para referirse a texto que ha sido codificado, encriptado. También, los expertos en el arte reconocerán que, no obstante el nombre, "texto claro" tiene la intencion de incluir, no solo datos textuales, sino también datos binarios, tanto en la forma de fichero, por ejemplo un fichero de ordenador, o en la forma de datos en serie que son transmitidos, por ejemplo, desde un sistema de comunicación, como en un sistema de satélites, un sistema telefónico, o un sistema de correo electrónico entre otros. También reconocerán que los términos "encriptación" y "cifrado", "encriptado" y "cifrado", "encriptador" y "cifrador", "desencriptador" y "descifrador", tienen un significado respectivamente equivalente en el arte, y pueden ser usados indistintamente a lo largo de la presente descripción.

Como es bien sabido por aquellos con conocimientos en el arte, hasta el momento un número amplio de esquemas de encriptación han sido usados. Hasta el momento actual todos los dispositivos de encriptación, entre los que se encuentran por mencionar algunos, como son, el dispositivo de encriptación "Data Encryption Standard" ("DES") del "American National Bureau of Standards", actual "National Institute of Standards and Technology" ("NBS" o "NIST") de Estados Unidos, el dispositivo de encriptación "Fast data encipherment algorithm FEAL" (FEAL) desarrollado en Japón posteriormente, IECEJ Technical Report IT 86-33 (1986) y objeto de la patente estadounidense número 4,850,019 de título "Data Randomization Equipment" del 18 de Julio de 1989, el dispositivo de encriptación conocido por el nombre de nombre IDEA, el cual es objeto de la patente estadounidense número 5,214,703 de título "Device for the conversion of a digital block and use of same" del 25 de Mayo de 1993, así como el dispositivo de encriptación objeto de la patente estadounidense número 5,675,653 de título "Method and apparatus for digital encryption" del 7 de Octubre de 1997, tras llevar a cabo la encriptación o cifrado de un texto claro siempre han delegado la fortaleza de la invulnerabilidad ante ataques enemigos por descubrir el contenido del texto cifrado o la clave con la que ha sido cifrado, que es al fin y al cabo el fin de los mencionados dispositivos, en la confianza que ha de delegar el usuario, o elemento que haga uso de él, en organismos, instituciones o expertos que avalan la confusión y difusión que introduce el dispositivo de encriptación utilizado en el texto cifrado. El usuario o elemento que realiza la encriptación, de un texto claro en particular, no tiene una medida de la confusión y difusión de valores presente en el texto cifrado resultado de la aplicación del dispositivo de encriptación.

Anteriormente se ha aducido una aleatorización de un bloque de datos de entrada como es el caso del dispositivo objeto de la patente estadounidense número 4,850,019 de título "Data randomization equipment", del 18 de Julio de 1989, cuyos inventores son Yokosuka Akihiro Shimizu y Yokohama Shoji Miyaguchi, ambos de Japón, en que se presentan dos encriptadores de texto claro. El primer dispositivo se describe a partir de la columna 7 línea 40 de la descripción de la referida patente, siendo las figuras del mismo las número 8 y 9, y el segundo dispositivo en la columna 8 línea 36 de la descripción de la referida patente, siendo las figuras del mismo las número 10 y

11. En ambos casos la aleatorización de datos a la que se refieren es respecto al bloque individual de 64 bits que se da como datos de entrada de los encriptadores de las figuras 8 y 10, y como se describe desde la columna 1, línea 67, a la línea 2 de la columna 2, de la descripción de la patente en que está explicitado que "Datos finales obtenidos del canal después de las operaciones funcionales y transformadoras son combinados por medios combinatorios para producir datos aleatorizados correspondientes a los datos de entrada". Las propiedades y características de dicha aleatorización residen en el bloque de datos de entrada, la clave de encriptación, y en las operaciones y transformaciones que realiza el dispositivo sobre el bloque de 64 bits en particular suministrado como datos de entrada. Se puede además mencionar que la referida invención hace uso como clave de encriptación, en el primero de los encriptadores, de 64 bits de datos de clave, como es mostrado en la figura 9 y es descrito en la columna 7, línea 46 de la descripción de la patente; y en el segundo de los encriptadores hace uso como clave de encriptación de 128 bits de datos de clave, como se muestra en la figura 11 y es descrito en la columna 8, desde la línea 38 a la línea 41 de la descripción de la patente.

El dispositivo de encriptación conocido por el nombre de IDEA, objeto de la patente estadounidense número 5,214,703 de título "Device for the conversion of a digital block and use of same", del 25 de Mayo de 1993, es otro encriptador que también hace gala de usar conocidas técnicas de confusión, difusión, etcétera, tal como está explicitado en las líneas 33 a 35 de la columna 1 de la descripción de la mencionada patente, así como en las líneas 3 a 5 de la columna 5 de la misma descripción de la mencionada patente; pero el texto cifrado resultado de su aplicación no presenta propiedades tales que hagan mesurables, por parte del usuario o elemento que lo utiliza, la confusión y difusión que presenta el mencionado texto cifrado, y al igual que el anterior dispositivo referenciado, se trata de confusión y difusión introducidas en el bloque de 64 bits. Se hace mención en las líneas 1 a 3 de la columna 5 de la descripción de la mencionada patente que "puede ser probado de que la cantidad de cuatro operaciones es un mínimo para alcanzar el objetivo de difusión", y por lo tanto también relegando en expertos, organismos o instituciones, el valorar la difusión y confusión que son introducidos en el texto cifrado resultado de su aplicación. La clave utilizada para realizar la encriptación tiene influencia en la difusión y confusión

presente en el texto cifrado resultado, tal como es reconocido desde la línea 67 de la columna 4 a la línea 1de la columna 5 de la descripción de la referida patente; así como en las líneas 22 a 25 y líneas 29 a 34 de la columna 6 de la misma descripción. Pero no se genera una confusión y difusión tal que se pueda presentar un modo de poder discernir entre diferentes textos encriptados resultado de la aplicación de diferentes claves de encriptación, que pueden ser usadas, a un mismo texto claro de entrada objeto de la encriptación, cual es el texto encriptado resultado que presenta mas difusión y confusión entre todos ellos; y por lo tanto, poder elegir el texto encriptado resultado y la clave de encriptación que ha producido ese texto encriptado resultado que presenta más difusión y confusión.

Otro ejemplo de dispositivo de encriptación en que se aduce una buena mezcla ("scramble" en el texto original en inglés de la descripción de la patente) en el texto encriptado resultado es el dispositivo objeto de la patente estadounidense número 5,675,653 de título "Method and apparatus for digital encryption", cuyo inventor es Nelson Douglas Valmore, Jr, del 7 de Octubre de 1997. En la mencionada patente se hace referencia también el hecho de que los expertos, las personas que tengan conocimientos en el arte de la encriptación, reconocerán que las técnicas típicas de encriptación digital generalmente utilizan dos bien conocidas técnicas, substitución y transposición, pero tampoco el dispositivo da como resultado un texto encriptado tal que sea factible medir la "mezcla" conseguida en el texto encriptado resultado de un modo objetivo y utilizable por los legos en la materia en cada una de las encriptaciones que realicen.

También cabe decir que respecto a la clave de encriptación que se usa para llevar a cabo la encriptación, hasta este momento, existen recomendaciones sobre como debe ser la mísma. Dichas recomendaciones son del tipo de las que se pueden encontrar en la publicación Federal Information Processing Standards Publication 112 o FIPS PUB 112, que anuncia el standard "Password usage" ("Uso de la palabra de paso"), del 30 de Mayo de 1985, del "National Institute of Standards and Technology" ("NIST") del Departamento de Comercio del Gobierno de los Estados Unidos. Las mencionadas recomendaciones son referentes a longitud del "password" o "palabra de paso", carácteres con los que es mejor que esté compuesta la "palabra de paso", y diferentes

limitaciones en la composición de la "palabra de paso", entre otras. Los entendidos en el arte reconocerán que las "palabras de paso" en muchas ocasiones tienen una relación, ya sea esta relación directa o indirecta, con las claves de encriptación y muchas veces son usadas como tales, tal como se recomienda en la misma publicación FIPS PUB 112 en diferentes secciones, como en la sección o punto 3.9.3 de título "Transmission" ("Transmisión") del capítulo 3 de título "Acceptable Basic Criteria" ("Criterios Básicos Aceptables"); otra referencia en el mismo sentido se puede encontrar en el punto o sección 3.7 de título "Storage" ("Almacenamiento") del capitulo 3 de título "Factors" ("Factores") del Apéndice A de título "Password Usage Guidelines" ("Guía de uso de la palabra de paso") y en otros puntos del mencionado documento.

Cuando se tiene que la clave de encriptación utilizada es elemento base transformador del texto claro en la encriptación del texto claro, puesto que son la combinación de las operaciones, más las propias operaciones que realiza el encriptador con el texto claro y la clave de encriptación lo que nos da el texto encriptado. Tenemos que la clave de encriptación utilizada es elemento transformador, diferenciador y variable de la serie de transformaciones que sufre el texto claro para producir el texto encriptado resultado. Como elemento base transformador del texto claro, la clave de encriptación tiene influencia en la confusión y difusión que presenta el texto encriptado, por lo que de entre todas las claves que se pueden utilizar, existen unas que introducirán más confusión y difusión de valores en el texto encriptado resultado que otras. Hasta el momento no se ha presentado un dispositivo de encriptación que pueda dar, como texto encriptado resultado de su aplicación, un texto tal que exista una manera mesurable y objetiva de discernir entre diferentes claves de encriptación que se pueden usar, cual o cuales producen mayor difusión y confusión en los textos encriptados resultado de la encriptación con cada una de las usadas claves de encriptación.

La confusión y difusión que presente el texto cifrado resultado, depende de la combinación de texto claro y clave de encriptación. Diferentes textos encriptados resultado de la encriptación de diferentes textos claros con una misma clave de encriptación presentarán diferente difusión y confusión de valores en el texto encriptado resultado respectivo de cada texto claro; así como un mismo texto claro

que se encripte con diferentes claves de encriptación, presentará en cada uno de los respectivos textos encriptados resultado un grado de difusión y confusión diferente.

Por lo tanto, se puede indicar que hasta el momento se ha dado el mismo valor de invulnerabilidad de un texto encriptado, resultado de la aplicación de un dispositivo de encriptación, a todos los posibles textos encriptados resultado que fuesen encriptados con distintas claves de encriptación basándose en la opinión de expertos en cuanto a la difusión y confusión que introducen los dispositivos de encriptación utilizados. Los dispositivos de encriptación hasta el momento no dan como resultado de su aplicación a un texto claro un texto encriptado resultado que presente substancialmente tales propiedades que permitan realizar una medición de la confusión y difusión objetiva presente en el texto encriptado resultado.

Cada vez es más amplia la utilización de los dispositivos de encriptación por parte de legos en el arte de la encriptación, como ocurre por ejemplo con las transacciones comerciales electrónicas, o el correo electrónico entre otros, en los que aquellas personas legas en el arte de la encriptación necesitan poder tener por ellos mismos una medida objetiva de la confusión y difusión presente en los datos encriptados. El poder disponer de un dispositivo de encriptación que de como resultado de su aplicación un texto encriptado tal que el lego en el arte de la encriptación pueda tener una medida objetiva de la confusión y difusión de valores, permitiría que los legos en el arte de la encriptación puedan tener una mayor seguridad en la confidencialidad de la información encriptada y por lo tanto usar con más confianza los dispositivos de encriptación; ésto ayudaría a que tengan una mayor aceptación y a un consiguiente incremento de uso, potenciándose con ello las comunicaciones de datos, correo electrónico y transacciones comerciales electrónicas entre otros.

Así mismo, respecto a la clave de encriptación usada, como se ha mencionado previamente, se realizan una serie de recomendaciones como las especificadas en el anteriormente mencionado Federal Information Processing Standards Publication 112 del 30 de Mayo de 1985 o FIPS PUB 112 del "National Institute of Standards and Technology" ("NIST") del Departamento de Comercio del Gobierno de los Estados Unidos, en que todas las posibles combinaciones de valores utilizables como clave de encriptación que cumplan con las recomendaciones expuestas son aceptables. No existe la posibilidad de discernir que clave de encriptación introduce más confusión y

difusión, más seguridad,en el texto cifrado, debido a la no existencia de un dispositivo de encriptación cuyo texto encriptado, resultado de la combinación de texto claro y clave de encriptación usada, presente substancialmente unas propiedades tales en que la confusión y difusión sean mesurables objetivamente y por lo tanto permita discriminar entre diferentes claves de encriptación, que se pueden probar, cuales producen un texto encriptado resultado en que esté presente una mayor difusión y confusión de valores.

Como se ha mencionado anteriormente aquellos entendidos en el arte de la encriptación reconocerán que es propósito de los dispositivos de encriptación introducir en el texto claro que se desea encriptar suficiente difusión y confusión de modo que no sea factible deducir a partir del texto cifrado resultado el texto claro objeto de la encriptación o la clave de encriptación utilizada para realizar la encriptación. Así mismo, aquellos con conocimientos en el arte de los generadores de secuencias de números aleatorios, arte muy relacionado con el arte de la encriptación, reconocerán que en las secuencias de números aleatorios se da un gran grado de difusión y confusión de valores, y además tienen la propiedad de que a partir de valores presentes en la secuencia no son deducibles otros valores de la misma. Para poder evaluar dichas secuencias de números aleatorios numerosos tests han sido presentados, como en "The Art of Computer Programming – 2ª Edicion" Volumen 2 "Seminumerical Algorithms", autor Donald E. Knuth, Addison-Wesley Publishing Company, ISBN: 0-201-03822-6(v.2) en las páginas 54 a 65; o los tests obligatorios descritos en el Federal Information Processing Standards Publication 140-1 o FIPS PUB 140-1, de título "Security requirements for cryptographic modules" ("Requisitos de seguridad para módulos criptográficos"), del 11 de Enero de 1994 , del "National Institute of Standards and Technology" ("NIST") del Departamento de Comercio del Gobierno de los Estados Unidos, en la sección 4.11.1 de título "Power-Up Tests", o "Tests de arranque"; tests a que deben ser sometidos los generadores de secuencias de números aleatorios a ser utilizados en módulos criptográficos gubernamentales del citado país. Aunque como se describe en la anteriormente mencionada publicación "The Art of Computer Programming – 2ª Edicion" Volumen 2 "Seminumerical Algorithms" autor Donald E. Knuth, Addison-Wesley Publishing Company ISBN: 0-201-03822-6(v.2) en la página 35 líneas 13 a 18, el hecho de que aunque una

secuencia se comporte aleatoriamente con respecto a tests T_1, T_2,...,T_n, no permite asegurar que no falle al aplicarla al test T_{n+1}; pero cada test de aleatoriedad aplicado dará más y más confianza en la aleatoriedad de la secuencia y por lo tanto en la confusión y difusión de valores presente en la secuencia. Por lo que el hecho de disponer de un dispositivo de encriptación tal que el texto encriptado resultado de su utilización presentase substancialmente las propiedades de las secuencias de números aleatorios permitiría aplicar de un modo computacionalmente factible tests de aleatoriedad, como los anteriormente mencionados, al texto encriptado resultado y por lo tanto tener una medida objetiva de la difusión y confusión presentes en cada texto encriptado en particular resultado de la encriptación. Los legos en el arte de la encriptación podrían tener, para cada texto encriptado por ellos mismos, una medida objetiva de la difusión y confusión presentes en el texto encriptado, lo que les infundiría más confianza en la confidencialidad de la información. Además si se da el caso de que una clave de encriptación utilizada con una secuencia de texto claro, no generase lo que se pudiese considerar suficiente difusión y confusión en el texto aleatorizado-encriptado resultado, sin demérito de las recomendaciones usuales de "palabras de paso" o claves de encriptación como las comentadas anteriormente, podría someterse al texto claro a un nuevo proceso de encriptación, con una clave de encriptación diferente, hasta que la confusión y difusión logradas fuesen las deseadas.

EXPLICACION DE LA INVENCION

La presente invención es un dispositivo para la aleatorización-encriptación de texto claro que va a ser transmitido a través de un medio, por un canal de transmisión o comunicaciones por ejemplo, en el cual puede ser visto, analizado o interceptado. Por ejemplo, y sin limitar lo precedente, un canal de transmisón o comunicación puede incluir una red de ordenadores, líneas de sistemas telefónicos terrestres, o celulares, una transmisión vía satélite, un disco de ordenador, y cualquier otro tipo de medio que puede ser utilizado para la transferencia de datos en forma digital. Como se utiliza aquí, "canal de transmisión" simplemente significa el medio sobre el que datos digitales son transportados.

En vista de las cuestiones que plantea el actual estado de la técnica, el objeto de la presente invención es suministrar un dispositivo de encriptación de datos tal que la

secuencia de datos de salida no solo esté encriptada o cifrada, sino que esté aleatorizada de tal modo que permite evaluar la confusión y difusión que presenta la secuencia de datos encriptados de salida con la clave de encriptación utilizada.

Aunque la técnica que se entiende como "cifrador de flujos", descrita en la página 589 a 592 del libro "Redes de ordenadores" Segunda Edición, autor Andrew S. Tanenbaum, editado por "Prentice-Hall Hispanoamericana, S.A.", ISBN: 968-880-176-3, y otros modos similares, como los descritos en la publicación Federal Information Processing Standards Publication 81 o FIPS PUB 81, que anuncia el standard "DES Modes of Operation" ("Modos de operación del DES"), del "National Institute of Standards and Technology" ("NIST") del Departamento de Comercio del Gobierno de los Estados Unidos, son hace tiempo utilizados en el arte de la encriptación, no ha sido notado que generen secuencias substancialmente aleatorias a las cuales les fuese computacionalmente factible la aplicación de tests de aleatoriedad como los anteriormente referenciados.

El dispositivo de la presente invención consigue los propósitos de generación de secuencias de datos encriptados substancialmente aleatorizadas haciendo uso del encriptador o codificador de bloques conocido por el nombre de IDEA, objeto de la patente estadounidense número 5,214,703 de título "Device for the conversion of a digital block and use of same", del 25 de Mayo de 1993; además permite hacer uso de una clave de encriptación de longitud más larga. Hace computacionalmente factible aplicar tests de aleatoriedad a la secuencia de datos aleatorizados-encriptados de salida, y con ello dar una medida objetiva de la confusión y difusión de valores que presenta la secuencia de datos aleatorizados-encriptados; y por lo tanto también tener una medida objetiva de la confusión y difusión de valores que introduce en el texto aleatorizado-encriptado la clave de encriptación utilizada para realizar la encriptación.

De acuerdo a la invención, el dispositivo consta de medios para recibir por primera entrada una secuencia de datos y de medios para recibir por segunda entrada un bloque de control. El bloque de control por medios de división es dividido en dos bloques iniciales de control, bloque inicial de control de longitud N y bloque inicial de control de longitud 2N. Medios lógicos generan subbloques de control de longitud M con el bloque inicial de control de longitud 2N. Medios ensambladores ensamblan bloques de datos de longitud N de la secuencia de datos suministrada por primera entrada. Por medios de agrupación se agrupa el bloque inicial de control de longitud

N y el bloque de datos de longitud N dando un interbloque de longitud N. El interbloque de longitud N se suministra como entrada del dispositivo de encriptación conocido por IDEA, objeto de la patente estadounidense número 5,214,703 de título "Device for the conversion of a digital block and use of same", del 25 de Mayo de 1993, donde es agrupado con los subbloques de control de longitud M, dando un bloque de salida de longitud N. El bloque de salida de longitud N se suministra como bloque inicial de control de longitud N para la aleatorización-encriptación del siguiente bloque de datos de longitud N y también se suministra como salida del dispositivo de aleatorización-encriptación objeto de la presente invención.

Medios de salida son proporcionados para transmitir la secuencia de datos aleatorizada-encriptada formada por los bloques de salida de longitud N, correspondientes a la secuencia de datos que se ha suministrado por primera entrada.

El propósito de la presente invención se puede alcanzar también con un dispositivo que consta de medios para recibir por primera entrada una secuencia de datos y de medios para recibir por segunda entrada un bloque de control. Medios lógicos generan subbloques de control de longitud M con el bloque de control. Medios ensambladores ensamblan bloques de datos de longitud N de la secuencia de datos suministrada por primera entrada. Constando el dispositivo de un bloque inicial de control de longitud N. Por medios de agrupación se agrupa el bloque inicial de control longitud N y el bloque de datos de longitud N dando un interbloque de longitud N. El interbloque de longitud N se suministra como entrada del dispositivo de encriptación conocido por IDEA, objeto de la patente estadounidense número 5,214,703 de título "Device for the conversion of a digital block and use of same", del 25 de Mayo de 1993, donde es agrupado con los subbloques de control de longitud M, dando un bloque de salida de longitud N. El bloque de salida de longitud N, se suministra para sustituir al bloque inicial de control de longitud N para la aleatorización-encriptación del siguiente bloque de datos de longitud N, y también se suministra como salida del dispositivo de aleatorización-encriptación objeto de la presente invención.

Medios de salida son proporcionados para transmitir la secuencia de datos aleatorizada-encriptada formada por los bloques de salida de longitud N, correspondientes a la secuencia de datos que se ha suministrado por primera entrada.

DESCRIPCION DE LAS FIGURAS

La FIG.1 muestra arte previo de un diagrama básico de enlazado de bloques de un sistema para la transmisión y tratamiento de datos en forma encriptada.

La FIG.2 muestra arte previo de diagrama de cableado de bloques del encriptador en el caso de una encriptación de bloque paso a paso, objeto de la patente estadounidense número 5,214,703, de título "Device for the conversion of a digital block and use of same", del 25 de Mayo de 1993, mostrada para referencias posteriores de la presente invención

La FIG.3 muestra arte previo de diagrama de cableado de bloques del encriptador en el caso de una encriptación de bloque paso a paso, objeto de la patente estadounidense número 5,214,703 de título "Device for the conversion of a digital block and use of same", esquematizado con respecto al representado en la FIG.2, con elementos relevantes de la mísma para la realización de la presente invención.

La FIG.4 muestra arte previo de diagrama de cableado de bloques del desencriptador en el caso de una desencriptación de bloque paso a paso, objeto de la patente estadounidense número 5,214,703 de título "Device for the conversion of a digital block and use of same", esquematizado con respecto al representado en la FIG.2, con elementos relevantes de la mísma para la realización de la presente invención.

La FIG.5 muestra diagrama básico del enlazado de bloques de un sistema para la transmisión de datos en forma aleatorizada-encriptada haciendo uso de los dispositivos de aleatorización-encriptación y desencriptación objetos de la presente invención.

La FIG.6 muestra diagrama básico de enlazado de bloques del dispositivo para aleatorización-encriptación de un mensaje de texto claro de acuerdo con la presente invención.

La FIG.7 muestra diagrama básico de enlazado de bloques del dispositivo para la desencriptación de un_mensaje de texto aleatorizado-encriptado con dispositivo de acuerdo con la presente invención

La FIG.8 muestra diagrama básico de enlazado de bloques de variante del dispositivo para aleatorización-encriptación de un mensaje de texto claro de acuerdo con la presente invención.

La FIG.9 muestra diagrama básico de enlazado de bloques de variante del dispositivo para la desencriptación de un mensaje de texto aleatorizado-encriptado con dispositivo de acuerdo con la presente invención.

MODOS DE REALIZACION

FIG.1 muestra arte previo de un diagrama básico de enlazado de bloques de un sistema para la transmisión y tratamiento de datos en forma encriptada. Pretende mostrar cual es hasta el momento el sistema generalmente utilizado. Los datos (texto claro $\underline{X}$) a ser transmitidos son originados en una fuente de mensaje 101, por ejemplo un ordenador. Estos datos son encriptados en un encriptador 102 y transmitidos como texto encriptado $\underline{Y}$ por una línea de transmisión de comunicaciones 103. El texto encriptado $\underline{Y}$ llega al desencriptador 104 en el lado del receptor el cual alimenta al destino 105, por ejemplo un segundo ordenador, con los datos $\underline{X}$ de forma desencriptada.

Para la encriptación y desencriptación de los datos, el encriptador 102 y el desencriptador 104 usan un bloque de clave de encriptación Z, el cual se suministra por medio de una fuente de clave 106, y por medio de un canal 107 a la unidad 102 y por un canal seguro 108 a la unidad 104. Este canal seguro 108 es por ejemplo un correo con un cubrimiento sellado.

El texto encriptado $\underline{Y}$ en el canal de transmisión 103 está siempre expuesto al riesgo de que un criptoanálisis enemigo 109, que leerá también este texto $\underline{Y}$, intentará obtener el texto claro $\underline{X}$ correspondiente o el bloque clave de encriptación Z (los resultados de estos intentos están designados por $\hat{\underline{X}}$ y $\hat{Z}$).

Hasta el momento la ocultación del contenido de texto claro $\underline{X}$ que está en el mensaje encriptado $\underline{Y}$ que se transmite por el canal de transmisión 103 reside en la avalada confusión y difusión introducida por el encriptador usado ante criptoanálisis enemigos 109, sea cual sea la clave de encriptación Z usada.

FIG.2 muestra diagrama de cableado de bloques del cifrador 102 en el caso de una encriptación de bloque paso a paso, descrita en la patente estadounidense número 5,214,703 de título "Device for the conversion of a digital block and use of same" del 25 de Mayo de 1993, que se corresponde con la FIG.2 de los dibujos de la referida

patente, y mostrada para referencias posteriores de realización de la presente invención. En la FIG.2, partes correspondientes a partes de la FIG.1 son designadas por mismas referencias numéricas, y referencias alfabéticas utilizadas son mismas referencias alfabéticas que se usan en la mencionada FIG.2 y descripción de la patente estadounidense número 5,214,703, de título "Device for the conversion of a digital block and use of same", de modo que sea más sencillo conocer el objeto de las referencias. El texto claro $\underline{X}$ a ser encriptado llega continuamente de la fuente de mensajes 101 a la unidad de entrada 201, por ejemplo un convertidor serie/paralelo en el caso de una fuente de bits serie. Paso a paso, esta unidad 201 ensambla bloques de texto claro X de longitud preferentemente N=64 bits, los cuales son particionados en cuatro subbloques X1, X2, X3, X4 cada uno de M=16 bits. Estos subbloques de texto claro de los respectivos bloques de texto claro X alcanzan una primera etapa 205.1 por primeras entradas 210 a 213, cada una formada por 16 líneas paralelas. En esta etapa 205.1, los subbloques X1 a X4 son agrupados juntos con seis subbloques de control diferentes por medio de funciones lógicas apropiadas. Durante el proceso de encriptación, los bloques de control (general) son subbloques clave Z_1 a Z_6 (especiales) y durante el proceso de desencriptación son subbloques de desencriptación U_1 a U_6, los cuales son derivados del bloque clave Z. El proceso de encriptación es descrito seguidamente, el término subbloque de control es preferido para referirse a los subbloques clave.

Los subbloques de control Z_1 a Z_6 están conectados a segundas entradas 240, 241, 242, 243, 244, 245 de la primera etapa de encriptación 205.1. Los dichos subbloques Z_1 a Z_6, así como los subbloques adicionales Z_7 a Z_{52}, son generados por la unidad de generación de subbloques de control 202. Esta unidad 202 recibe, por el canal seguro 107, el bloque clave o bloque de control Z deseado que preferentemente forma una secuencia de L=128 bits.

El método para la obtención de dichos subbloques de control Z_1 a Z_{52} utilizados en el proceso de encriptación del bloque de control Z por la unidad de generación de subbloques de control 202 es así mismo descrito en la descripción de la mencionada patente estadounidense número 5,214,703 de título "Device for the conversion of a digital block and use of same" y haciendo uso de mismas referencias alfanuméricas. De aquí en adelante esta misma nomenclatura de subbloques de control Z_1 a Z_{52} será utilizada para hacer referencia a los subbloques clave en el proceso de encriptación.

Los subbloques de control Z_1 a Z_6 están conectados a las anteriormente mencionadas seis segundas entradas 240, 241, 242, 243, 244, 245 de la primera etapa de encriptación 205.1. El resultado del agrupamiento en esta etapa 205.1 aparece en las cuatro salidas o conexiones 220 a 223, específicamente como primeros cuatro intersubbloques W11, W12, W13, W14 de M=16 bits en cada instancia, los cuales juntos forman un primer intersubbloque W1 de longitud N=64 bits.

Los primeros intersubbloques W11 a W14 están conectados a las conexiones o entradas 220 a 223 (idénticas a las salidas de la etapa precedente 205.1) de una segunda etapa de encriptación 205.2 para el segundo paso de encriptación . Esta etapa de encriptación 205.2 está construida de forma que es idéntica a la etapa de encriptación 205.1. Los subbloques de control Z_7 a Z_{12} descritos están conectados a sus seis segundas entradas de control, y los segundos intersubbloques W21, W22, W23, W24 o el segundo intersubbloque W2 en su totalidad, aparece en sus salidas.

Los segundos intersubbloques W21 a W24 están conectados a una tercera etapa de encriptación, no mostrada, para el tercer paso de encriptación; los tercer intersubbloques W31 a W34 están conectados a una cuarta etapa de encriptación, etcétera, hasta una novena etapa de encriptación 206, la cual es diferente a las etapas precedentes y comprende cuatro segundas entradas 288, 289, 290, 291.

Finalmente, cuatro subbloques de texto cifrado Y1, Y2, Y3, Y4 de longitud M=16 bits, los cuales juntos forman un bloque de texto encriptado Y, el cual se corresponde al bloque de texto claro X, aparece en las salidas 230 a 233 de la novena etapa 206. Este bloque de texto encriptado Y es convertido en una unidad de salida 203, por ejemplo un convertidor paralelo/serie, de tal forma que puede ser transmitido por la línea de transmisión 103.

El proceso de encriptación es por lo tanto efectuado en nueve etapas de encriptación sucesivas 205.1, 205.2, 206, las primeras ocho de las cuales son idénticas. Todos los 52 diferentes subbloques de control Z_1 a Z_{52} antes mencionados sirven como clave. La unidad de encriptación-desencriptación 204 necesaria para el proceso de encriptación --X->Y está indicada como línea discontinua en la FIG.2.

FIG.3 muestra diagrama de cableado de bloques del encriptador en el caso de una encriptación de bloque paso a paso como es descrita en la previamente mencionada patente estadounidense número 5,214,703, de título "Device for the conversion of a

digital block and use of same", esquematizado con respecto al representado en la FIG.2 de la presente, con elementos relevantes para la descripción de la presente invención. En la FIG.3, partes correspondientes a partes de la FIG.1 y FIG.2 son designadas por mismas referencias numéricas y alfabéticas. La FIG.3 muestra un diagrama de cableado de bloques del cifrador 102. El texto claro $\underline{X}$ a ser cifrado llega continuamente de la fuente de mensajes 101 a la unidad ensambladora de entrada 301, por ejemplo un convertidor serie/paralelo en el caso de una fuente de bits serie. Paso a paso, esta unidad ensambladora de entrada 301 ensambla bloques de texto claro X de longitud preferentemente N=64 bits. Los subbloques de texto claro X1, X2, X3, X4 de la FIG.2 juntos forman el bloque de texto claro X mostrado en la FIG.3. Este bloque de texto claro llega a la unidad de encriptación-desencriptación 204 por primera entrada 312, formada por 64 líneas paralelas. La primera entrada 312 es la agrupación de las cuatro primeras entradas 210 a 213, formadas por 16 líneas paralelas cada una, mostradas en la FIG.2. Durante el proceso de encriptación, los bloques de control (general) son subbloques de control Z_1 a Z_{52} (especiales) derivados del bloque de control Z en la unidad de generación de subbloques de control 202, tal como se ha especificado en la descripción de la FIG.2. Los subbloques de control Z_1 a Z_{52} llegan a la unidad de encriptación-desencriptación 204 por segunda entrada 311. La segunda entrada 311 representa la agrupación de las 52 entradas secundarias 240 a 291 de la unidad de encriptación-desencriptación 204 de la FIG.2. Finalmente, un bloque de texto cifrado Y, el cual se corresponde al bloque de texto claro X, aparece en la salida 313 de la unidad de encriptación-desencriptación 204. La salida 313 de la unidad de encriptación-desencriptación 204 está formada por 64 líneas paralelas, y es la agrupación de las cuatro salidas 230 a 233, de 16 líneas paralelas cada una, de la FIG.2. Este bloque de texto cifrado Y es convertido en una unidad de salida 302 por ejemplo un convertidor paralelo/serie, de tal forma que puede ser transmitido por la línea de transmisión 103.

FIG.4 muestra diagrama de cableado de bloques del descifrador en el caso de una desencriptación de bloque paso a paso como es descrita en la patente estadounidense número 5,214,703 de título "Device for the conversion of a digital block and use of same", esquematizado con respecto al representado en la FIG.2 de la presente, con elementos relevantes para la descripción de la presente invención. En la FIG.4, partes

correspondientes a partes de la FIG.1 y FIG.2 son designadas por mismas referencias numéricas y alfabéticas. La FIG.4 muestra un diagrama de cableado de bloques del descifrador 104. El texto encriptado $\underline{Y}$ a ser descifrado llega continuamente de la línea de transmisión 103 a la unidad ensambladora de entrada 301, por ejemplo un convertidor serie/paralelo en el caso de una fuente de bits serie. Paso a paso, esta unidad ensambladora de entrada 301 ensambla bloques de texto encriptado Y de longitud preferentemente N=64 bits. El bloque de texto encriptado Y es agrupación de cuatro subbloques Y1, Y2, Y3, Y4, cada uno de longitud M=16 bits mostrados en la FIG.2. Este bloque de texto cifrado Y llega a la unidad de encriptación-desencriptación 204, idéntica a la unidad de encriptación-desencriptación 204 de las FIG.2 y FIG.3, por primera entrada 312, formada por 64 líneas paralelas. La primera entrada 312 de la unidad de encriptación-desencriptación 204 es agrupación de cuatro primeras entradas 210 a 213, de 16 líneas paralelas cada una, de la FIG.2.

Durante el proceso de desencriptación, los bloques de control (general) son subbloques de control U_1 a U_{52} (especiales) derivados del bloque de control Z en la unidad de generación de subbloques de control 401, tal como se describe en la descripción de la mencionada patente estadounidense número 5,214,703 de título "Device for the conversion of a digital block and use of same" haciendo uso de las mismas referencias alfanuméricas. De aquí en adelante esta misma nomenclatura de subbloques de control U_1 a U_{52} será utilizada para hacer referencia a los subbloques clave U_1 a U_{52} en el proceso de desencriptación.

Los subbloques de control U_1 a U_{52} llegan a la unidad de encriptación-desencriptación 204 por segunda entrada 311. La segunda entrada 311 es agrupación de cincuenta y dos entradas secundarias 240 a 291 de la unidad de encriptación-desencriptación 204 de la FIG.2. Finalmente, un bloque de texto claro X de la primera longitud N=64 bits, el cual se corresponde al bloque de texto cifrado Y, aparece en la salida 313, formada por 64 líneas paralelas, de la unidad de encriptación-desencriptación 204. La salida 313 de la unidad de encriptación-desencriptación 204 es agrupación de cuatro salidas 230 a 233, de 16 líneas paralelas cada una, de la FIG.2 Este bloque de texto claro X es convertido en una unidad de salida 302, por ejemplo un convertidor paralelo/serie, de tal forma que puede ser transmitido a la unidad destino 105.

FIG.5 muestra diagrama básico de uno de los posibles enlazados de bloques de un dispositivo para la transmisión de datos en forma aleatorizada-encriptada haciendo uso de los dispositivos de aleatorización-encriptación y desencriptación objeto de la presente invención. En la FIG.5, partes correspondientes a partes de la FIG.1 son designadas por mismas referencias numéricas. Los datos (texto claro X) a ser transmitidos son originados en una fuente de mensaje 101, por ejemplo un ordenador. Estos datos son aleatorizados-encriptados en un aleatorizador-encriptador 501 haciendo uso de un bloque de clave de aleatorización-encriptación Kp, que se suministra por medio de una fuente de clave 504 y por medio del canal 107 a la unidad de aleatorización-encriptación 501, dando como resultado un texto aleatorizado-encriptado Yp candidato a ser transmitido por una línea de transmisión de comunicaciones 103.

El texto aleatorizado-encriptado Yp, entre una de las múltiples configuraciones del sistema posibles, en el caso de una transmisión del texto aleatorizado-encriptado Yp por un canal de comunicaciones, como se muestra en la FIG.5, se puede pasar por un canal 505 a una unidad emisor de mensajes 506, a la espera del resultado de la aplicación de los tests de aleatoriedad en la unidad analizador de aleatoriedad 503.

Dadas las substanciales propiedades de las secuencias aleatorias que presenta el texto aleatorizado-encriptado Yp generado en la unidad aleatorizador-encriptador 501 es sometible a un analisis de aleatoriedad (en analizador de aleatoriedad 503) para tener conocimiento del cumplimiento por parte del texto aleatorizado-encriptado Yp de las mencionadas propiedades correspondientes a las secuencias aleatorias, y tener una medida objetiva de la confusión y difusión que presenta el texto aleatorizado-encriptado Yp. El resultado de la aplicación de los tests de aleatoriedad en la unidad analizador de aleatoriedad 503 al texto aleatorizado-encriptado Yp es designado como Tp. Conocido el resultado Tp, resultado de la aplicación del analizador de aleatoriedad 503 a la secuencia de texto aleatorizado-encriptado Yp, se informa del resultado Tp a la fuente de la clave 504.

El mencionado analizador de aleatoriedad 503 puede ser una implementación hardware o software de una selección o la totalidad de diferentes tests de aleatoriedad existentes, como descritos en "The Art of Computer Programming – 2ª Edicion" Volumen 2 "Seminumerical Algorithms" autor Donald E. Knuth, Addison-Wesley Publishing Company, ISBN: 0-201-03822-6(v.2) en las páginas 54 a 65, o los tests

obligatorios descritos en el Federal Information Processing Standards Publication 140-1 o FIPS PUB 140-1, de título "Security requirements for cryptographic modules" ("Requisitos de seguridad para módulos criptográficos"), del 11 de Enero de 1994, del "National Institute of Standards and Technology" ("NIST") del Departamento de Comercio del Gobierno de los Estados Unidos, en la sección 4.11.1 de título "Power-Up Tests", o "Tests de arranque", a que deben ser sometidos los generadores de secuencias de números aleatorios a ser utilizados en módulos criptográficos gubernamentales del citado país. Como se describe en la anteriormente mencionada publicación "The Art of Computer Programming – 2ª Edicion" Volumen 2 "Seminumerical Algorithms", autor Donald E. Knuth, Addison-Wesley Publishing Company ISBN: 0-201-03822-6(v.2) en la página 35, líneas 13 a 18, el hecho de que una secuencia se comporte aleatoriatoriamente con respecto a tests T_1, T_2,...,T_n, no se puede asegurar que no falle al aplicarla al test T_{n+1}; pero cada test de aleatoriedad aplicado dará más y más confianza en la aleatoriedad de la secuencia, y por lo tanto en la confusión y difusión de valores presente en la secuencia de texto aleatorizada-encriptada Yp; siendo punto abierto los tests de aleatoriedad específicos que se implementen en el analizador de aleatoriedad 503 para ser aplicados.

Con el resultado Tp del analizador de aleatoriedad 503 la fuente de clave 504 puede llevar a cabo dos acciones. Uno, puede decidir la transmisión del texto aleatorizado-encriptado Yp, por el canal de transmisión 103 como texto aleatorizado-encriptado seleccionado Ys, representado por medio de la señal S de envío del texto aleatorizado-encriptado Yp que contiene la unidad emisor de mensaje encriptado 506, y proveer la clave de aleatorización-encriptación Kp utilizada por medio del canal seguro 108 como clave de aleatorización-encriptación seleccionada Ks, usada para la aleatorización-encriptación del texto claro X, al descifrador 502. Dos, puede decidir seleccionar una nueva clave de aleatorización-encriptación Kp, someter al mensaje de texto claro X a nueva aleatorización-encriptación en la unidad de aleatorización-encriptación 501, y someter el nuevo mensaje de texto aleatorizado-encriptado Yp al analizador de aleatoriedad 503 y actuar según el nuevo resultado Tp de aleatoriedad.

El texto aleatorizado-encriptado Ys, que es el texto aleatorizado-encriptado Yp seleccionado que es transmitido, llega al desencriptador 502 en el lado del receptor. El desencriptador 502 alimenta al destino 105, por ejemplo un segundo ordenador, con el texto claro X desencriptado.

Para la desencriptación de los datos, el desencriptador 502 usa el bloque de clave de aleatorización-encriptación seleccionado Ks que se suministra por medio de la fuente de clave 504 por medio de un canal seguro 108 a la unidad 502. Este canal seguro 108 es por ejemplo un correo con un cubrimiento sellado.

El texto aleatorizado-encriptado Ys en el canal de transmisión 103 está siempre expuesto al riesgo de que un criptoanálisis enemigo 109 leerá también este texto Ys e intentara obtener el texto claro X correspondiente o el bloque clave de aleatorización-encriptación Ks (los resultados de estos intentos están designados por $\hat{X}$ y $\hat{Ks}$).

En los dispositivos de encriptación existentes hasta el momento la confusión y difusión de valores que presenta el mensaje cifrado Y que se transmite por el canal de transmisión 103 reside en la confusión y difusión, avalada por expertos, instituciones u organismos, que introduce el algoritmo de encriptación usado, sea cual sea la clave de encriptación usada; pero los textos encriptados Y particulares resultado de su aplicación no presentan características tales que sea computacionalmente factible tener una medida objetiva y referencial de la confusión y difusión de los valores que componen el texto cifrado Y que se transmite. Con la presente invención el dispositivo de cifrado da como resultado de su aplicación texto cifrado tan substancialmente aleatorizado, que además de poder basar la difusión y confusión presente en el texto aleatorizado-encriptado Ys en el aval hoy por hoy existente en el algoritmo de encriptación conocido por IDEA, objeto de la patente estadounidense número 5,214,703 de título "Device for the conversion of a digital block and use of same", sobre el que se apoya el dispositivo descrito en la presente invención, permite poder tener una medida objetiva de la confusión y difusión de valores presente en un texto aleatorizado-encriptado Ys particular resultado de una aleatorización-encriptación de un texto claro X particular con una clave de aleatorización-encriptación Ks particular. De tal modo que además permite diferenciar entre diferentes claves de aleatorización-encriptación Kp, la difusión y confusión que generan en el texto aleatorizado-encriptado Yp, y por lo tanto tener la posibilidad de elección de aquella que de más seguridad subjetiva en cuanto a la resistencia del mensaje aleatorizado-encriptado Ys ante criptoanálisis enemigos.

FIG.6 muestra diagrama básico de enlazado de bloques del dispositivo para aleatorización-encriptación de un mensaje de texto claro de acuerdo con la invención.

En la FIG.6, partes correspondientes a partes de las FIG.1, FIG.3 y FIG.5 son designadas por mismas referencias alfanuméricas. El bloque de clave o bloque de control Kp, de longitud preferentemente F=192 bits llega por canal 107, alcanzando unidad divisora de bloque de control 601, que presenta dos salidas 610 y 611. Salida 610 formada por 64 líneas paralelas y salida 611 formada por 128 líneas paralelas. La unidad divisora de bloque de control 601 divide el bloque de control Kp en dos bloques iniciales de control Z y W. Los términos bloque de control y subbloque de control es preferido para referirse a los bloque de clave y subbloques de clave. Siendo el bloque inicial de control Z de longitud preferentemente L1=128 bits, y el bloque inicial de control W de longitud preferentemente L2=64 bits. El bloque inicial de control Z se suministra a unidad de generación de subbloques de control 202 por salida 611, la unidad de generación de subbloques de control 202 genera subbloques de control Z_1 a Z_{52}, de longitud M=16 bits cada uno, que se suministran por entrada secundaria 311 de la unidad de encriptación-desencriptación 204. El subbloque inicial de control W se suministra a unidad 602, la cual puede ser implementada por ejemplo con un registro, por salida 610. La unidad 602, presenta entradas 610 y 614, y salida 613, formada cada una de ellas por 64 líneas paralelas, siendo el propósito de la unidad 602 contener el bloque WI de longitud N=64 bits que se suministra como entrada de la unidad de agrupación 603 por entrada 613.

El texto claro $\underline{X}$ a ser cifrado llega continuamente de la fuente de mensajes 101 a la unidad ensambladora de entrada 301, por ejemplo un convertidor serie/paralelo en el caso de una fuente de bits serie. Paso a paso, esta unidad ensambladora de entrada 301 ensambla bloques de texto claro XI de longitud preferentemente N=64 bits. La unidad ensambladora de entrada 301 tiene salida 612, que es entrada de unidad de agrupación 603. La unidad de agrupación 603 presenta dos entradas 612 y 613, de 64 líneas paralelas cada una, y salida 312, también de 64 líneas paralelas. En la unidad de agrupación 603 se agrupan los bloques XI y WI, ambos de longitud N=64 bits que llegan por entradas 612 y 613 respectivamente, generando un interbloque VI de longitud N=64 bits.

La operación de agrupación que se realiza en la unidad de agrupación 603 es la conocida OR-exclusiva o XOR bit a bit tal como es conocida desde el mencionado standard DES, de tal modo que $XI \oplus WI \rightarrow VI$. Seguidamente se presenta la TABLA

1 donde se muestra la tabla de verdad de la mencionada operación XOR para el caso de bloque de longitud de 1 bit únicamente como muestra de la operación de la misma.

TABLA 1
OPERACIÓN XOR

XI	WI	Resultado XI ⊕ WI → VI
0	0	0
0	1	1
1	0	1
1	1	0

Este interbloque VI alcanza la unidad de encriptación-desencriptación 204 por primera entrada 312, formada por 64 líneas paralelas. En esta unidad de encriptación-desencriptación 204, el interbloque VI es agrupado junto con los cincuenta y dos subbloques de control Z_1 a Z_{52}, de longitud M=16 bits cada uno, generados por la unidad de generación de subbloques de control 202 y que llegan por segunda entrada 311.

Finalmente, un bloque de texto aleatorizado-encriptado YI de longitud N=64 bits, aparece en la salida 313 de la unidad de encriptación-desencriptación 204. La salida 313, formada por 64 líneas paralelas, está conectada a la unidad de salida 302 y por entrada 614 a la unidad 602. La entrada 614 tiene como una de múltiples implementaciónes, el ser una derivación de la salida 313. El bloque de texto aleatorizado-encriptado YI por la salida 313 alcanza la unidad de salida 302 y también el mismo bloque de texto aleatorizado-encriptado YI se suministra a la unidad 602 por entrada 614 para ser utilizado como bloque WI en la aleatorización-encriptación del siguiente bloque de texto claro XI que será ensamblado en la unidad ensambladora de entrada 301 en el siguiente paso de aleatorización-encriptación.

Este bloque de texto cifrado YI puede ser convertido en una unidad de salida 302, por ejemplo un convertidor paralelo/serie, de tal forma que puede ser transmitido por la línea de transmisión 505. Todos los bloques YI juntos forman el texto aleatorizado-encriptado Yp.

La unidad 602 que en la FIG.6 muestra entradas 610 y 614, y salida 613, de 64 líneas paralelas cada una, contiene para el primer bloque de texto claro XI, de todo el texto claro X que es ensamblado en la unidad ensambladora de entrada 301, el bloque

inicial de control W, y para los siguientes, segundo en adelante bloques de texto claro XI, el bloque de texto aleatorizado-encriptado YI resultado de la encriptación del anterior bloque de texto claro XI. En la siguiente TABLA 2 se muestran los diferentes valores que adquiere el bloque WI para los diferentes y sucesivos bloques de texto claro XI de un texto claro X que es aleatorizado-encriptado; siendo el bloque de texto aleatorizado-encriptado YI_1 el resultado de la aleatorización-encriptación del primer bloque de texto claro XI_1, el bloque de texto aleatorizado-encriptado YI_2 el resultado de la aleatorización-encriptación del segundo bloque de texto claro XI_2, y así sucesivamente.

TABLA 2
VALORES QUE ADQUIERE WI

Orden de bloque de texto claro que es aleatorizado-encriptado	Bloque de texto claro que es aleatorizado-encriptado	Bloque que contiene WI
Primero	XI_1	W
Segundo	XI_2	YI_1
Tercero	XI_3	YI_2
....	.....	....
N	XI_n	YI_{n-1}

Dado que el texto aleatorizado-encriptado Yp, resultado del proceso de aleatorización-encriptación presenta substancialmente las propiedades de las secuencias aleatorias, es sometible a un análisis de aleatoriedad (en analizador de aleatoriedad 503 de la FIG.5) para tener conocimiento del cumplimiento por parte del texto aleatorizado-encriptado Yp de las propiedades consustanciales de las secuencias aleatorias y así tener una medida objetiva y referencial de la confusión y difusión que presenta el texto aleatorizado-encriptado Yp. Conocido el resultado Tp de la aplicación de los tests de aleatoriedad en la unidad analizador de aleatoriedad 503 al texto aleatorizado-encriptado Yp, de cumplimiento o no de dichas propiedades de aleatoriedad, puede decidirse entre enviar el texto aleatorizado-encriptado Yp, resultado de la aleatorización-encriptación realizada con la clave de aleatorización-encriptación Kp, por el canal de transmisión 103 mostrado en la FIG.5, y enviar la clave de aleatorización-encriptación Kp como clave de aleatorización-encriptación Ks por el canal seguro 108 mostrado en la FIG.5, o puede someterse al texto claro X a un nuevo proceso de encriptación con una nueva clave de aleatorización-encriptación Kp.

Dicha operación es computacionalmente factible por las mencionadas características de presentar el texto aleatorizado-encriptado Yp, resultado de la encriptación con la presente invención, substancialmente características propias de las secuencias aleatorias. Por lo que el dispositivo de la presente invención presenta la nueva posibilidad de poder medir objetivamente la confusión y difusión que presenta el texto aleatorizado-encriptado Yp particular por parte de legos en la materia, tener una medida para no expertos de la confusión y difusión presente en el texto aleatorizado-encriptado Yp; así como poder diferenciar entre diferentes, y cualesquiera que sean utilizadas, claves de aleatorización-encriptación Kp posibles, cual, o cuales, de ellas nos da, o dan, una mayor confusión y difusión de valores en el texto aleatorizado-encriptado resultado Yp particular.

Se tiene además que la longitud de la clave de aleatorización-encriptación Ks es formada por una secuencia de preferentemente 192 bits, y aunque es actualmente aceptado que 128 bits de longitud de clave de encriptación son suficientes ante ataques enemigos, cuanto mayor es la longitud en bits de la clave utilizada por el dispositivo de encriptación, más segura es la inviolabilidad del texto encriptado que se desea proteger.

Además, con el dispositivo de aleatorización-encriptación de acuerdo a la invención se tiene un generador de números aleatorios. Suministrando diferentes datos de entrada como texto claro X, texto Yp que forma una secuencia aleatoria es dada como salida. Estos datos de salida pueden ser referidos como datos numéricos aleatorios, o secuencia aleatoria. Esto significa que el dispositivo de aleatorización-encriptación de acuerdo a la invención puede ser usado también como un generador de números aleatorios.

Por la difusión y confusión del texto aleatorizado-encriptado resultado que presenta el dispositivo de aleatorización-encriptación de la presente invención, unido a la influencia que un cambio de un bit en el texto claro X de entrada conlleva en todos los bits posteriores de salida, puede el dispositivo de aleatorización-encriptación 501 también ser utilizado como "funcion de hash" o "funcion de encriptación en una direccion" ("one-way encryption") como es conocida por aquellos con conocimientos en el arte de la encriptación.

FIG.7 muestra diagrama básico de enlazado de bloques del dispositivo para la desencriptación de un mensaje de texto aleatorizado-encriptado de acuerdo con la

invención. En la FIG.7, partes correspondientes a partes de las FIG.1, FIG.4 y FIG.5 son designadas por mismas referencias alfanuméricas. El bloque de clave o bloque de control Ks, de longitud preferentemente F=192 bits llega por canal 108, alcanzando la unidad divisora de bloque de control 701, la cual presenta mencionada entrada 108 y salidas 710 y 711. La salida 710 formada por 64 líneas paralelas y la salida 711 formada por 128 líneas paralelas. La unidad divisora de bloque de control 701 es igual a la unidad divisora de bloque de control 601 de la FIG.6. La unidad divisora de bloque de control 701 divide el bloque de clave o bloque de control Ks en dos bloques iniciales de control Z y W. Los términos bloque de control y subbloque de control es preferido para referirse a los bloque de clave y subbloques de clave. Siendo el bloque inicial de control Z de longitud preferentemente de L1=128 bits, y el bloque inicial de control W de longitud preferentemente L2=64 bits. El bloque inicial de control Z se suministra a la unidad de generación de subbloques de control 401 por entrada 711, para que la unidad de generación de subbloques de control 401 genere subbloques de control U_1 a U_{52} que se suministran por entrada secundaria 311 a la unidad de encriptación-desencriptación 204. El bloque inicial de control W se suministra a la unidad 703, que puede ser implementada con un registro por ejemplo, por salida 710. La unidad 703, tiene entradas 710 y 713, formadas cada una de ellas por 64 líneas paralelas, y salida 714, formada también por 64 líneas paralelas. El propósito de la unidad 703 es contener el bloque WJ de longitud N=64 bits que se suministra como entrada de la unidad de agrupación 704 por entrada 714.

El texto aleatorizado-encriptado Ys a ser descifrado llega continuamente por el canal de transmisión 103 a la unidad ensambladora de entrada 301, por ejemplo un convertidor serie/paralelo en el caso de una fuente de bits serie. Paso a paso, esta unidad ensambladora de entrada 301 ensambla bloques de texto aleatorizado-encriptado YJ de longitud preferentemente N=64 bits. La unidad ensambladora de entrada 301 tiene salida 312, formada por 64 líneas paralelas, que conecta con la unidad de encriptación-desencriptación 204, y con la unidad 702, por entrada 712. La entrada 712 de la unidad 702 puede ser una derivación de la salida 312 y está también formada por 64 líneas paralelas. Una vez ensamblado el bloque de texto aleatorizado-encriptado YJ se suministra a la unidad de encriptación-desencriptación 204 y a la unidad 702 por salida 312.

La unidad 702 presenta entrada 712 y salida 713, cada una formada por 64 líneas paralelas. El propósito de la unidad 702 es mantener una copia del actual bloque de texto aleatorizado-encriptado YJ que se suministra como entrada de la unidad de encriptación-desencriptación 204 para una utilización posterior, la cual será descrita más adelante.

El bloque de texto aleatorizado-encriptado YJ alcanza la unidad de encriptación-desencriptación 204 por primera entrada 312, formada por 64 líneas paralelas. En esta unidad de encriptación-desencriptación 204, el bloque YJ es agrupado juntos con los cincuenta y dos subbloques de control U_1 a U_{52}, de longitud M=16 bits cada uno, generados por la unidad de generación de subbloques de control 401 y llegan por segunda entrada 311 a la unidad de encriptación-desencriptación 204.

Tras la agrupación del bloque de texto YJ y los subbloques de control U_1 a U_{52} en la unidad de encriptación-desencriptación 204, un bloque de texto SJ de longitud N=64 bits aparece en salida 313 de la unidad de encriptación-desencriptación 204. La salida 313 esta formada por 64 líneas paralelas, y es entrada de la unidad de agrupación 704.

La unidad de agrupación 704 consta de entradas 313 y 714, y salida 715, de 64 líneas paralelas cada una. En esta unidad de agrupación 704 se agrupan los bloques SJ y WJ, ambos de longitud N=64 bits que llegan por entradas 313 y 714 respectivamente, dando como salida un bloque de texto claro XJ de longitud N=64 bits. La operación de agrupación que se realiza en la unidad de agrupación 704 es la ya anteriormente descrita y conocida OR-exclusiva o XOR bit a bit de tal modo que $SJ \oplus WJ \rightarrow XJ$. La tabla de verdad de la mencionada operación XOR para el caso de bloque de longitud de 1 bit únicamente ha sido mostrada previamente en la TABLA 1.

Este bloque de texto claro XJ se suministra por salida 715, formada por 64 líneas paralelas, a la unidad de salida 302. Una vez se tiene el bloque de texto claro XJ, se carga la unidad 703 con el actual bloque YJ que contiene la unidad 702 por entrada 713, para que en la desencriptación del siguiente bloque YJ, la unidad 703 contenga como bloque WJ el bloque YJ que acaba de ser desencriptado.

El bloque de texto claro XJ es convertido en una unidad de salida 302, por ejemplo un convertidor paralelo/serie, de tal forma que puede ser transmitido a la unidad de destino 105, la cual obtiene el texto claro $\underline{X}$ tras realizarse todo el proceso con la secuencia $\underline{Ys}$.

La unidad 703 que en la FIG.7 muestra entradas 710 y 713, y salida 714, de 64 líneas paralelas cada una, contiene para el primer bloque de texto aleatorizado-encriptado YJ de todo el texto aleatorizado-encriptado Ys, que es ensamblado en la unidad ensambladora de entrada 301, el bloque inicial de control W, y para los siguientes, segundo en adelante, bloques de texto aleatorizado-encriptado YJ el anterior bloque de texto aleatorizado-encriptado YJ que ha sido previamente desencriptado. En la siguiente TABLA 3 se muestran los diferentes valores que adquiere el bloque WJ para los diferentes y sucesivos bloques de texto aleatorizado-encriptado YJ de un texto aleatorizado-encriptado Ys que es desencriptado.

TABLA 3
VALORES QUE ADQUIERE WJ

Orden de bloque de texto aleatorizado-encriptado que es desencriptado	Bloque de texto aleatorizado-encriptado que es desencriptado	Bloque que contiene WJ
Primero	YJ_1	W
Segundo	YJ_2	YJ_1
Tercero	YJ_3	YJ_2
....	.....	....
N	YJ_n	YJ_{n-1}

FIG.8 muestra diagrama básico de enlazado de bloques de variante del dispositivo de aleatorización-encriptación de un mensaje de texto claro de acuerdo con la invención. En la FIG.8, partes correspondientes a partes de las FIG.1, FIG.3, FIG.5 y FIG.6 son designadas por mismas referencias alfanuméricas. En esta variante del dispositivo de aleatorización-encriptación 501v, el bloque de clave Kpv, siendo Kpv variante de bloque de clave o bloque de control Kp, de longitud preferentemente F=128 bits llega por canal 107, alcanzando la unidad de generación de subbloques de control 202. En esta variante del dispositivo de aleatorización-encriptación 501v el bloque de control Kpv forma el bloque inicial de control Z mostrado en la descripción de la FIG.6. El bloque inicial de control Z, o Kpv, se suministra a la unidad de generación de subbloques de control 202 para que la unidad de generación de subbloques de control 202 genere subbloques de control Z_1 a Z_{52} que se suministran por entrada secundaria 311 de la unidad de encriptación-desencriptación 204. En esta variante del dispositivo de encriptación 501v la unidad 602v, que puede ser implementado con un registro por ejemplo, es una variante de la unidad 602 de la FIG.6; en esta variante presenta

entrada 614, y salida 613, formadas cada una de ellas por 64 líneas paralelas, aunque igual que la unidad 602 de la FIG.6 el propósito de la unidad 602v es contener el bloque WI de longitud N=64 bits que se sumnistra como entrada de la unidad de agrupación 603 por entrada 613. Variante con respecto al dispositivo de aleatorización-encriptación 501 de la FIG. 6 es que la unidad 602v no se carga a partir del bloque de control Kpv con ningún bloque inicial de control W como en el dispositivo de aleatorización-encriptación 501 de la FIG.6; el primer bloque WI que se suministra por la salida 613 para ser agrupado con el primer bloque de texto claro XI en la unidad de agrupación 603 es un bloque inicial que contiene previamente la unidad 602v.

Al igual que en la unidad de aleatorización-encriptación 501 de la FIG.6 el texto claro $\underline{X}$ a ser aleatorizado-encriptado llega continuamente de la fuente de mensajes 101 a la unidad ensambladora de entrada 301, por ejemplo un convertidor serie/paralelo en el caso de una fuente de bits serie. Paso a paso, esta unidad ensambladora de entrada 301 ensambla bloques de texto claro XI de longitud preferentemente N=64 bits. La unidad ensambladora 301 tiene salida 612, que es entrada de la unidad de agrupación 603. La unidad de agrupación 603 presenta entradas 612 y 613, de 64 líneas paralelas cada una, y salida 312, también de 64 líneas paralelas. En la unidad de agrupación 603 se agrupan los bloques XI y WI, ambos de longitud N=64 bits que llegan por entradas 612 y 613 respectivamente, dando como salida un interbloque VI de longitud N=64 bits.

La operación de agrupación que se realiza en la unidad de agrupación 603 es la conocida OR-exclusiva o XOR bit a bit, de tal modo que $XI \oplus WI \rightarrow VI$. Anteriormente se ha mostrado la TABLA 1 donde se da la tabla de verdad de la mencionada operación XOR para el caso de bloque de longitud de 1 bit únicamente como muestra de la operación de la mísma.

Este interbloque VI alcanza la unidad de encriptación-desencriptación 204 por primera entrada 312, formada por 64 líneas paralelas. En esta unidad de encriptación-desencriptación 204, el interbloque VI es agrupado junto con los cincuenta y dos subbloques de control Z_1 a Z_{52}, de longitud M=16 bits cada uno, generados por la unidad de generación de subbloques de control 202 y que llegan por segunda entrada 311.

Finalmente, un bloque de texto aleatorizado-encriptado YI de longitud N=64 bits, aparece por la salida 313 de la unidad de encriptación-desencriptación 204. La salida 313, formada por 64 líneas paralelas, está conectada a la unidad de salida 302 y por entrada 614 a la unidad 602v. La entrada 614 tiene como una de múltiples implementaciónes el ser una derivación de la salida 313. El bloque de texto aleatorizado-encriptado YI por la salida 313 alcanza la unidad de salida 302 y también el mismo bloque de texto aleatorizado-encriptado YI se suministra a la unidad 602v por entrada 614 para ser utilizado como bloque WI en la aleatorización-encriptación del siguiente bloque de texto claro XI ensamblado en la unidad ensambladora de entrada 301 en la siguiente aleatorización-encriptación de bloque de texto claro XI.

Este bloque de texto aleatorizado-encriptado YI puede ser convertido en una unidad de salida 302, por ejemplo un convertidor paralelo/serie, de tal forma que puede ser transmitido por la línea de transmisión 505. Todos los bloques YI juntos forman el texto aleatorizado-encriptado Yp.

La unidad 602v que en la FIG.8 presenta entrada 614, y salida 613, de 64 líneas paralelas cada una, contiene para el primer bloque de texto claro XI de todo el texto claro X, que es ensamblado en la unidad ensambladora de entrada 301, un bloque inicial cualquiera de longitud N=64 bits, y para los siguientes, segundo en adelante, bloques de texto claro XI, el bloque de texto aleatorizado-encriptado YI resultado de la encriptación del anterior bloque de texto claro XI. En la siguiente TABLA 4 se muestran los diferentes valores que adquiere el bloque WI para los diferentes y sucesivos bloques de texto claro XI de un texto claro X que es aleatorizado-encriptado, siendo el bloque de texto aleatorizado-encriptado YI_1 el resultado de la aleatorización-encriptación del bloque de texto claro XI_1, el bloque de texto aleatorizado-encriptado YI_2 el resultado de la aleatorización-encriptación del bloque de texto claro XI_2, y así sucesivamente.

TABLA 4
VALORES QUE ADQUIERE WI

Orden de bloque de texto claro encriptado	Bloque de texto claro encriptado	Bloque que contiene WI
Primero	XI_1	Bloque inicial en unidad 602v
Segundo	XI_2	YI_1
Tercero	XI_3	YI_2
....	...	....
N	XI_n	YI_{n-1}

También en esta variante de la unidad de aleatorización-encriptación 501v dado que el texto aleatorizado-encriptado Yp, resultado del proceso de aleatorización-encriptación presenta substancialmente las propiedades de las secuencias aleatorias, es sometible a un análisis de aleatoriedad (en analizador de aleatoriedad 503 de la FIG.5) para tener conocimiento del cumplimiento por parte del texto aleatorizado-encriptado Yp de las propiedades asociadas a las secuencias aleatorias y así tener una medida de la confusión y difusión que presenta el texto aleatorizado-encriptado Yp. Conocido el resultado de la aplicación de los tests de aleatoriedad en la unidad analizador de aleatoriedad 503 de la FIG.5, al texto aleatorizado-encriptado Yp, de cumplimiento o no de dichas propiedades de aleatoriedad, puede decidirse entre enviar el texto aleatorizado-encriptado Yp, resultado de la encriptación realizada con la clave de aleatorización-encriptación Kpv, por el canal de transmisión 103 de la FIG.5, y enviar la clave de aleatorización-encriptación Kpv como clave de aleatorización-encriptación Ks por el canal seguro 108 de la FIG.5, o puede someterse al texto claro X a un nuevo proceso de encriptación con una nueva clave de aleatorización-encriptación Kpv.

Dicha operación es computacionalmente factible por las mencionadas características de presentar el texto aleatorizado-encriptado Yp, resultado de la aleatorización-encriptación con la presente variante de la invención, también substancialmente características propias de las secuencias aleatorias. Por lo que esta variante del dispositivo de la presente invención también presenta la nueva posibilidad de poder medir objetivamente la confusión y difusión que presenta el texto aleatorizado-encriptado Yp particular por parte de legos en la materia, tener una medida para no expertos de la confusión y difusión presente en el texto aleatorizado-encriptado Yp; así como poder diferenciar entre diferentes, y cualesquiera que sean, claves de aleatorización-encriptación Kpv posibles utilizables, cual, o cuales, de ellas nos da, o dan, una mayor confusión y difusión de valores en el texto aleatorizado-encriptado Yp resultado.

Aunque en esta variante 501v del dispositivo de encriptación 501 la clave de aleatorización-encriptación Kpv está formada por una secuencia de preferentemente 128 bits, siendo por lo tanto mas "débil" ante ataques enemigos, como puede ser un ataque por lo que los entendidos en el arte de la encriptación se denomina "fuerza bruta", que la clave de aleatorización-encriptación Kp usada en la unidad de

aleatorización-encriptación 501 de la FIG.6, es aceptado que actualmente 128 bits de longitud de clave presentan por el momento suficiente seguridad ante los mencionados ataques enemigos.

Además, al igual que el dispositivo de aleatorización-encriptación 501de la FIG.6, con la variante del dispositivo de aleatorización-encriptación 501v que se muestra en la FIG.8 se tiene un generador de secuencias de números aleatorios. Suministrando diferentes datos de entrada como texto claro X, texto Yp que forma una secuencia de números aleatoria es dada como salida. Estos datos de salida pueden ser referidos como datos numéricos aleatorios, o secuencia aleatoria. Esto significa que la variante del dispositivo de aleatorización-encriptación de acuerdo a la invención puede ser usado también como un generador de números aleatorios.

También, puede el dispositivo de aleatorización-encriptación 501v ser utilizado como "funcion de hash" o "funcion de encriptación en una direccion" ("one-way encryption") como es conocida por aquellos con conocimientos en el arte de la encriptación.

FIG.9 muestra diagrama básico de enlazado de bloques de una variante del dispositivo de desencriptación de un mensaje de texto aleatorizado-encriptado con variante mostrada en la FIG.8 de la presente invención. En la FIG.9, partes correspondientes a partes de las FIG.1, FIG.4, FIG.5 y FIG.7 son designadas por mismas referencias alfanuméricas. El bloque de clave Ksv en esta variante del dispositivo es de longitud preferentemente F=128 bits. El bloque de clave de desencriptación Ksv es el bloque de clave de aleatorización-encriptación Kpv de la FIG.8 seleccionado, correspondiente al texto cifado-aleatorizado Ys que llega por el canal de transmisión 103. El bloque de clave de desencriptación Ksv llega por el canal 108. En esta variante del dispositivo de desencriptación 502v el bloque de clave o bloque de control Ksv forma el bloque inicial de control Z mencionado en la descripción de la FIG.7. El bloque inicial de control Z, o Kpv, se suministra a la unidad de generación de subbloques de control 401 por el canal seguro 108, la unidad de generación de subbloques de control 401 genera subbloques de control U_1 a U_{52}, de longitud M=16 bits cada uno, a partir del bloque de control Z que se suministran por segunda entrada 311 a la unidad de encriptación-desencriptación 204.

La unidad 703v, tiene entrada 713 y salida 714, formada cada una de ellas por 64 líneas paralelas,. El propósito de la unidad 703v, que puede implementarse por ejemplo por medio de un registro, es contener el bloque WJ de longitud N=64 bits que se suministra como entrada de la unidad de agrupación 704 por entrada 714.

En esta variante del dispositivo de encriptación 502v la unidad 703v, es una variante de la unidad 703 de la FIG.7. Variante con respecto al dispositivo de desencriptación 502 de la FIG. 7 es que la unidad 703v no se carga a partir del bloque de clave Ksv con ningun bloque inicial de control W como en el dispositivo de desencriptación 502; el primer bloque WJ que se suministra por la salida 714 para ser agrupado con el primer bloque de texto SJ en la unidad de agrupación 704 es un bloque inicial que contiene previamente la unidad 703v, y que debe ser igual al bloque que contenía la unidad 602v de la unidad de aleatorización-encriptación 502v de la FIG.8 al inicio de la aleatorización-encriptación del texto claro X correspondiente al texto aleatorizado-encriptado Ys objeto de la actual desencriptación.

El texto aleatorizado-encriptado Ys a ser descifrado llega continuamente por el canal de transmisión 103 a la unidad ensambladora de entrada 301, por ejemplo un convertidor serie/paralelo en el caso de una fuente de bits serie. Paso a paso, esta unidad ensambladora de entrada 301 ensambla bloques de texto aleatorizado-encriptado YJ de longitud preferentemente N=64 bits. La unidad ensambladora de entrada 301 tiene salida 312, formada por 64 líneas paralelas, que conecta con la unidad de encriptación-desencriptación 204, y con la unidad 702, por entrada 712. La entrada 712 de la unidad 702, puede ser implementada como una derivación de la salida 312 y está también formada por 64 líneas paralelas. La unidad 702 pueder ser implementada entre múltiples opciones como un registro. Una vez ensamblado el bloque de texto aleatorizado-encriptado YJ se suministra a la unidad de encriptación-desencriptación 204 por salida 312 y a la unidad 702 por entrada 712.

La unidad 702 tiene entrada 712, y salida 713, cada una formada por 64 líneas paralelas. El propósito de la unidad 702 es mantener una copia del actual bloque de texto aleatorizado-encriptado YJ que se suministra como entrada de la unidad de encriptación-desencriptación 204 para una utilización posterior, la cual será descrita mas adelante.

El bloque de texto aleatorizado-encriptado YJ alcanza la unidad de encriptación-desencriptación 204 por primera entrada 312, formada por 64 líneas paralelas. En esta

unidad de encriptación-desencriptación 204, el bloque YJ es agrupado juntos con los cincuenta y dos subbloques de control U_1 a U_{52}, de longitud M=16 bits cada uno, generados por la unidad de generación de subbloques de control 401 y que llegan por segunda entrada 311 a la unidad de encriptación-desencriptación 204.

Tras la agrupación del bloque de texto YJ y los subbloques de control U_1 a U_{52} en la unidad de encriptación-desencriptación 204, un bloque de texto SJ de longitud N=64 bits aparece en la salida 313 de la unidad de encriptación-desencriptación 204. La salida 313 está formada por 64 líneas paralelas, y es entrada de la unidad de agrupación 704.

La unidad de agrupación 704 consta de entradas 313 y 714, y salida 715, de 64 líneas paralelas cada una. En esta unidad de agrupación 704 se agrupan los bloques SJ y WJ, ambos de longitud N=64 bits que llegan por entradas 313 y 714 respectivamente, dando como salida un bloque de texto claro XJ de longitud N=64 bits. La operación de agrupación que se realiza en la unidad de agrupación 704 es la ya anteriormente descrita y conocida OR-exclusiva o XOR bit a bit de tal modo que $SJ \oplus WJ \rightarrow XJ$. La tabla de verdad de la mencionada operación XOR para el caso de bloque de longitud de 1 bit únicamente ha sido mostrada previamente como TABLA 1.

Este bloque de texto claro XJ se suministra por salida 715, formada por 64 líneas paralelas, a la unidad de salida 302. Una vez se tiene el bloque de texto claro XJ, se carga la unidad 703v con el actual bloque YJ que contiene la unidad 702 por entrada 713, de modo que en la desencriptación del siguiente bloque YJ, la unidad 703v contiene como bloque WJ el bloque YJ que acaba de ser desencriptado.

El bloque de texto claro XJ es convertido en una unidad de salida 302, por ejemplo un convertidor paralelo/serie, de tal forma que puede ser transmitido a la unidad de destino 105, la cual obtiene el texto claro $\underline{X}$ tras realizarse todo el proceso con la secuencia $\underline{Ys}$.

La unidad 703v que en la FIG.9 muestra entrada 713, y salida 714, contiene para el primer bloque de texto aleatorizado-encriptado YJ, de todo el texto aleatorizado-encriptado $\underline{Ys}$ ensamblado en la unidad ensambladora de entrada 301, un bloque inicial de longitud N=64 bits igual al bloque que contenía la unidad 602v de la unidad de aleatorización-encriptación 501v al ser aleatorizado-encriptado el bloque de texto claro $\underline{X}$ para dar el texto aleatorizado-encriptado $\underline{Ys}$; y para los siguientes, segundo en adelante, bloques de texto aleatorizado-encriptado YJ el anterior bloque de texto

aleatorizado-encriptado YJ. En la siguiente TABLA 5 se muestran los diferentes valores que adquiere el bloque WJ según los diferentes y sucesivos bloques de texto aleatorizado-encriptado YJ de un texto aleatorizado-encriptado Ys que es desencriptado.

TABLA 5
VALORES QUE ADQUIERE WJ

Orden de bloque de texto aleatorizado-encriptado que es desencriptado	Bloque de texto aleatorizado-encriptado que es desencriptado	Bloque que contiene WJ
Primero	YJ_1	Bloque inicial en unidad 703v identico al bloque inicial de la unidad 602v de la FIG.8 con que se aleatorizó-encriptó el texto Ys
Segundo	YJ_2	YJ_1
Tercero	YJ_3	YJ_2
....	.....	....
N	YJ_n	YJ_{n-1}

La implementación específica de los dispositivos de aleatorización-encriptación y desencriptación, así como sus variantes, pueden ser realizados de diferentes modos y pueden depender en varios factores como la aplicación que se hará de los mismos, el entorno, la tecnología usada y accesible, etcétera. Una implementación software que se ejecute en computadores electrónicos puede ser dada. Por otra parte, una implementación hardware puede ser también dada en la que las funciones lógicas elementales están en forma de unidades de circuitos independientes que pueden ser construidos de elementos chip discretos o preferentemente de varios módulos de integracion en gran escala ("very large scale integration o VLSI"); microprocesadores usando Memoria Solo de Lectura ("Read Only Memory" o "ROM"), o Memoria Solo de Lectura Programable ("Programmable Read Only Memory" o "PROM"), o Memoria Solo de Lectura Electrónicamente Borrable ("Electronically Erasable Read Only Memory" o "EEROM"); entre muchas implementaciones posibles. La implementación hardware tiene la ventaja sobre la implementación software que puede trabajar substancialmente mas rápido.

REIVINDICACIONES

1. Dispositivo de aleatorización-encriptación de secuencia de datos que haciendo uso de bloque de control libremente seleccionable con mencionada secuencia de datos genera una secuencia substancialmente aleatoria caracterizado por incluir:

medios de primera entrada para recibir secuencia de datos,

medios de segunda entrada para recibir bloque de control,

medios ensambladores de bloques de datos de longitud N que ensambla bloque de datos de longitud N con mencionada secuencia de datos recibida por mencionados medios de primera entrada,

medios divisores de bloque de control que dividen mencionado bloque de control recibido por mencionados medios de segunda entrada en dos bloques iniciales de control, bloque inicial de control de longitud N y bloque inicial de control de longitud 2N,

medios para contener mencionado bloque inicial de control de longitud N dividido en mencionados medios divisores de bloque de control,

medios generadores de subbloques de control de longitud M que generan subbloques de control de longitud M con mencionado bloque inicial de control de longitud 2N,

medios agrupadores que agrupan mencionado bloque de datos de longitud N con mencionado bloque inicial de control de longitud N, generando interbloque de longitud N,

medios de encriptación que agrupan mencionado interbloque de longitud N con mencionados subbloques de control de longitud M, generando bloque de salida de longitud N, donde mencionados medios de encriptación incluyen dispositivo de encriptación objeto de la patente estadounidense número 5,214,703 de título "Device for the conversion of a digital block and use of same",

medios para reemplazar mencionado bloque inicial de control longitud N con mencionado bloque de salida de longitud N,

medios de salida que agrupan mencionado bloque de salida de longitud N formando secuencia de datos aleatorizados-encriptados de salida correspondiente a mencionada secuencia de datos recibida por mencionados medios de primera entrada.

2. Dispositivo de acuerdo con la reivindicación 1 caracterizado porque mencionados medios agrupadores de mencionado bloque de datos de longitud N con mencionado bloque inicial de control de longitud N, generando mencionado interbloque de longitud N, incluyen operación OR-exclusiva.

3. Dispositivo de acuerdo con la reivindicación 2 caracterizado por mencionados medios generadores de subbloques de control de longitud M incluyen unidad generadora de subbloques de clave de encriptación descrita en patente estadounidense número 5,214,703 de título "Device for the conversion of a digital block and use of same".

4. Dispositivo de acuerdo con la reivindicación 3 caracterizado por mencionado bloque de control formado preferentemente por 192 bits.

5. Dispositivo de recuperación de secuencia de datos aleatorizados-encriptados con dispositivo de reivindicación 1 que haciendo uso de bloque de control libremente seleccionable a partir de la secuencia de datos aleatorizados-encriptados recupera secuencia de datos a partir de los cuales fueron generados caracterizado por incluir:

medios de primera entrada para recibir secuencia de datos aleatorizados-encriptados,

medios de segunda entrada para recibir bloque de control,

medios ensambladores de bloques de datos aleatorizados-encriptados de longitud N que ensambla bloque de datos aleatorizados-encriptados de longitud N de mencionada secuencia de datos aleatorizados-encriptados recibida por mencionados medios de primera entrada,

medios divisores de bloque de control que dividen mencionado bloque de control recibido por mencionados medios de segunda entrada en dos bloques iniciales de control, bloque inicial de control de longitud N y bloque inicial de control de longitud 2N,

medios para contener mencionado bloque inicial de control de longitud N dividido en mencionados medios divisores de bloque de control,

medios generadores de subbloques de control de longitud M que generan subbloques de control de longitud M con mencionado bloque inicial de control de longitud 2N,

medios de desencriptación que agrupan mencionado bloque de datos aleatorizados-encriptados de longitud N con mencionados subbloques de control de longitud M,

generando interbloque de longitud N, donde mencionados medios de desencriptación incluyen dispositivo de desencriptación objeto de la patente estadounidense número 5,214,703 de título "Device for the conversion of a digital block and use of same",

medios agrupadores que agrupan mencionado interbloque de longitud N con mencionado bloque inicial de control de longitud N, generando bloque de salida de longitud N,

medios para reemplazar mencionado bloque inicial de longitud N con mencionado bloque de datos aleatorizados-encriptados de longitud N,

medios de salida que agrupan mencionado bloque de salida de longitud N formando secuencia de datos de salida correspondiente a mencionada secuencia de datos aleatorizados-encriptados recibida por mencionados medios de primera entrada.

6. Dispositivo de acuerdo con la reivindicación 5 caracterizado porque mencionados medios agrupadores de mencionado interbloque de longitud N con mencionado bloque inicial de control de longitud N, generando mencionado bloque de salida de longitud N, incluyen operación OR-exclusiva.

7. Dispositivo de acuerdo con la reivindicación 6 caracterizado por mencionados medios generadores de subbloques de control de longitud M incluyen unidad generadora de subbloques de clave de desencriptación descrita en patente estadounidense número 5,214,703 de título "Device for the conversion of a digital block and use of same".

8. Dispositivo de acuerdo con la reivindicación 7 caracterizado por mencionado bloque de control formado preferentemente por 192 bits.

9. Dispositivo de aleatorización-encriptación de secuencia de datos que haciendo uso de bloque de control libremente seleccionable con mencionada secuencia de datos genera una secuencia substancialmente aleatoria caracterizado por incluir:

medios de primera entrada para recibir secuencia de datos,

medios de segunda entrada para recibir bloque de control,

medios ensambladores de bloques de datos de longitud N que ensambla bloque de datos de longitud N con mencionada secuencia de datos recibida por mencionados medios de primera entrada,

medios para contener bloque inicial de control de longitud N,

medios generadores de subbloques de control de longitud M que generan subbloques

de control de longitud M con mencionado bloque de control,

medios agrupadores que agrupan mencionado bloque de datos de longitud N con mencionado bloque inicial de control de longitud N, generando interbloque de longitud N,

medios de encriptación que agrupan mencionado interbloque de longitud N con mencionados subbloques de control de longitud M, generando bloque de salida de longitud N, donde mencionados medios de encriptación incluyen dispositivo de encriptación objeto de la patente estadounidense número 5,214,703 de título "Device for the conversion of a digital block and use of same",

medios para reemplazar mencionado bloque inicial de longitud N con mencionado bloque de salida de longitud N,

medios de salida que agrupan mencionado bloque de salida de longitud N formando secuencia de datos aleatorizados-encriptados de salida correspondiente a mencionada secuencia de datos recibida por mencionados medios de primera entrada.

10. Dispositivo de acuerdo con la reivindicación 9 caracterizado porque mencionados medios agrupadores de mencionado bloque de datos de longitud N con mencionado bloque inicial de control de longitud N, generando mencionado interbloque de longitud N, incluyen operación OR-exclusiva.

11. Dispositivo de acuerdo con la reivindicación 10 caracterizado por mencionados medios generadores de subbloques de control de longitud M incluyen unidad generadora de subbloques de clave de encriptación descrita en patente estadounidense número 5,214,703 de título "Device for the conversion of a digital block and use of same".

12. Dispositivo de acuerdo con la reivindicación 11 caracterizado por mencionado bloque de control formado preferentemente por 128 bits.

13. Dispositivo de recuperación de secuencia de datos aleatorizados-encriptados con dispositivo de la reivindicación 7 que haciendo uso de bloque de control libremente seleccionable a partir de la secuencia de datos aleatorizados-encriptados recupera secuencia de datos a partir de los cuales fueron generados caracterizado por incluir:

medios de primera entrada para recibir secuencia de datos aleatorizados-encriptados,

medios de segunda entrada para recibir bloque de control,

medios ensambladores de bloques de datos aleatorizados-encriptados de longitud N que ensamblan bloque de datos aleatorizados-encriptados de longitud N de mencionada secuencia de datos aleatorizados-encriptados recibida por mencionados medios de primera entrada,

medios para contener bloque inicial de control de longitud N,

medios generadores de subbloques de control de longitud M que generan subbloques de control de longitud M con mencionado bloque de control,

medios de desencriptación que agrupan mencionado bloque de datos aleatorizados-encriptados de longitud N con mencionados subbloques de control de longitud M, generando interbloque de longitud N, donde mencionados medios de desencriptación incluyen dispositivo de desencriptación objeto de la patente estadounidense número 5,214,703 de título "Device for the conversion of a digital block and use of same",

medios agrupadores que agrupan mencionado interbloque de longitud N con mencionado bloque inicial de control de longitud N, generando bloque de salida de longitud N,

medios para reemplazar mencionado bloque inicial de longitud N con mencionado bloque de datos aleatorizados-encriptados de longitud N,

medios de salida que agrupan mencionado bloque de salida de longitud N formando secuencia de datos de salida correspondiente a mencionada secuencia de datos aleatorizados-encriptados recibida por mencionados medios de primera entrada.

14. Dispositivo de acuerdo con la reivindicación 13 caracterizado porque mencionados medios agrupadores de mencionado interbloque de longitud N con mencionado bloque inicial de control de longitud N, generando mencionado bloque de salida de longitud N, incluyen operación OR-exclusiva.

15. Dispositivo de acuerdo con la reivindicación 14 caracterizado por mencionados medios generadores de subbloques de control de longitud M incluyen unidad generadora de subbloques de clave de desencriptación descrito en patente estadounidense número 5,214,703 de título "Device for the conversion of a digital block and use of same".

16. Dispositivo de acuerdo con la reivindicación 15 caracterizado por mencionado bloque de control formado preferentemente por 128 bits.

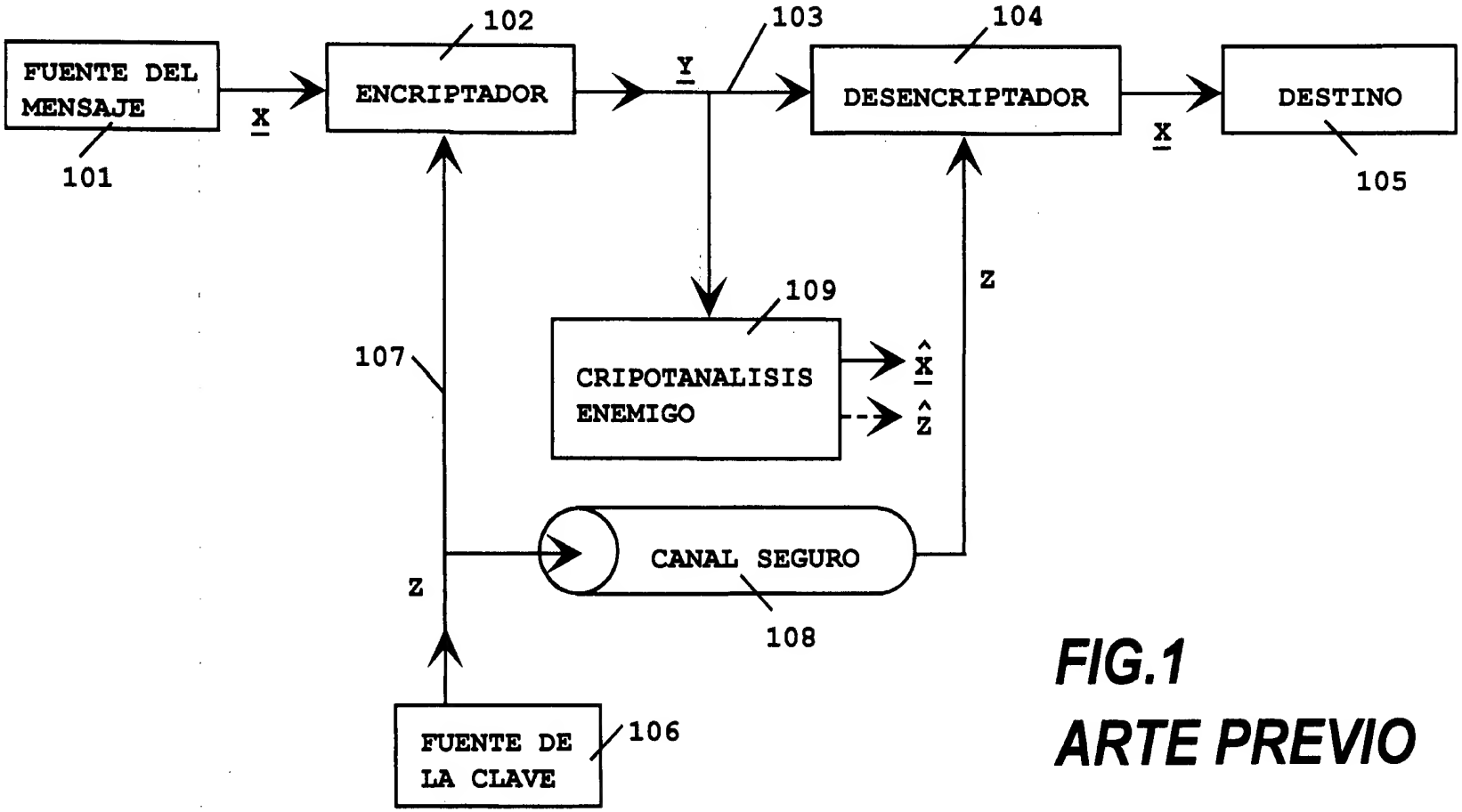

FIG.1
ARTE PREVIO

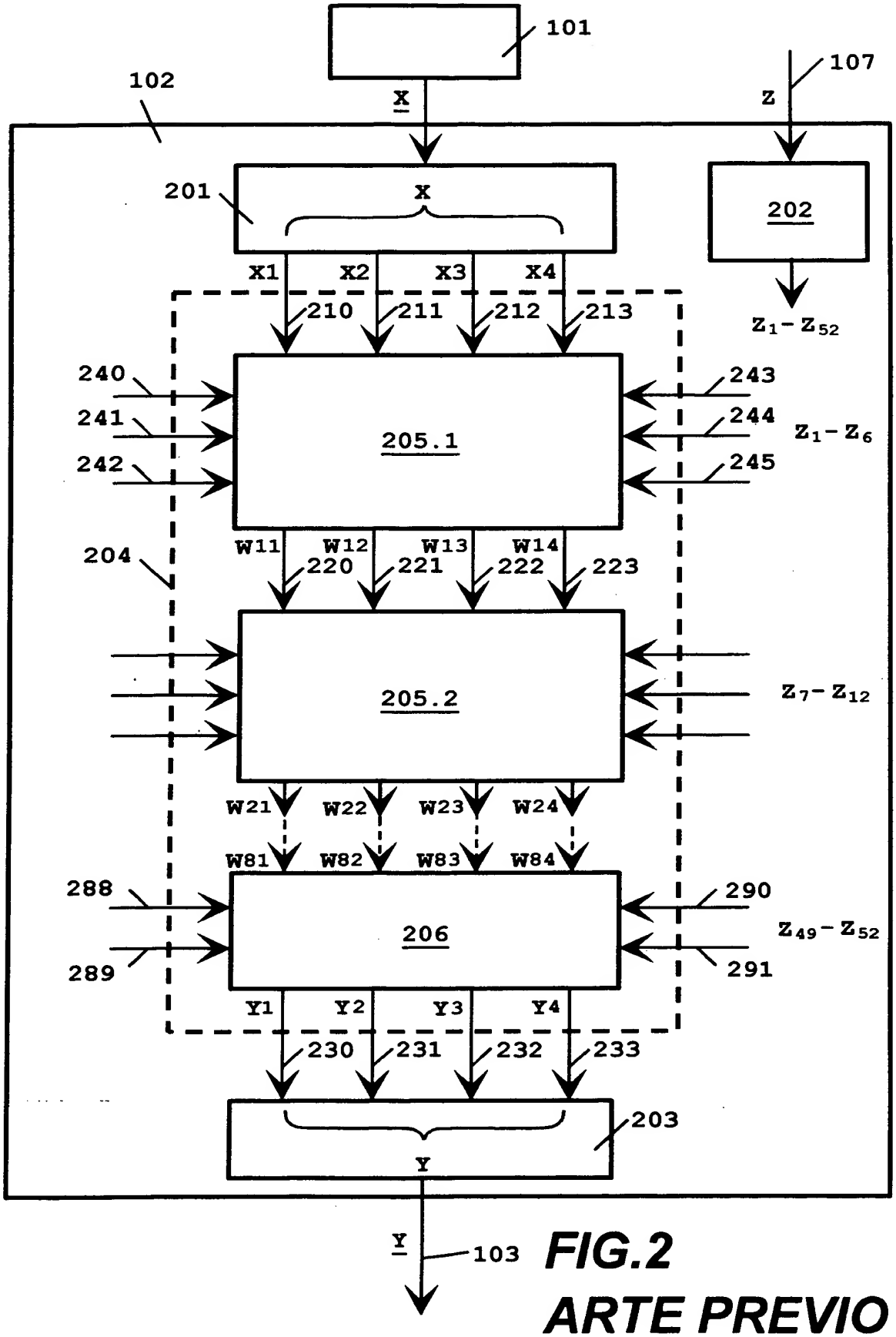

FIG.2
ARTE PREVIO

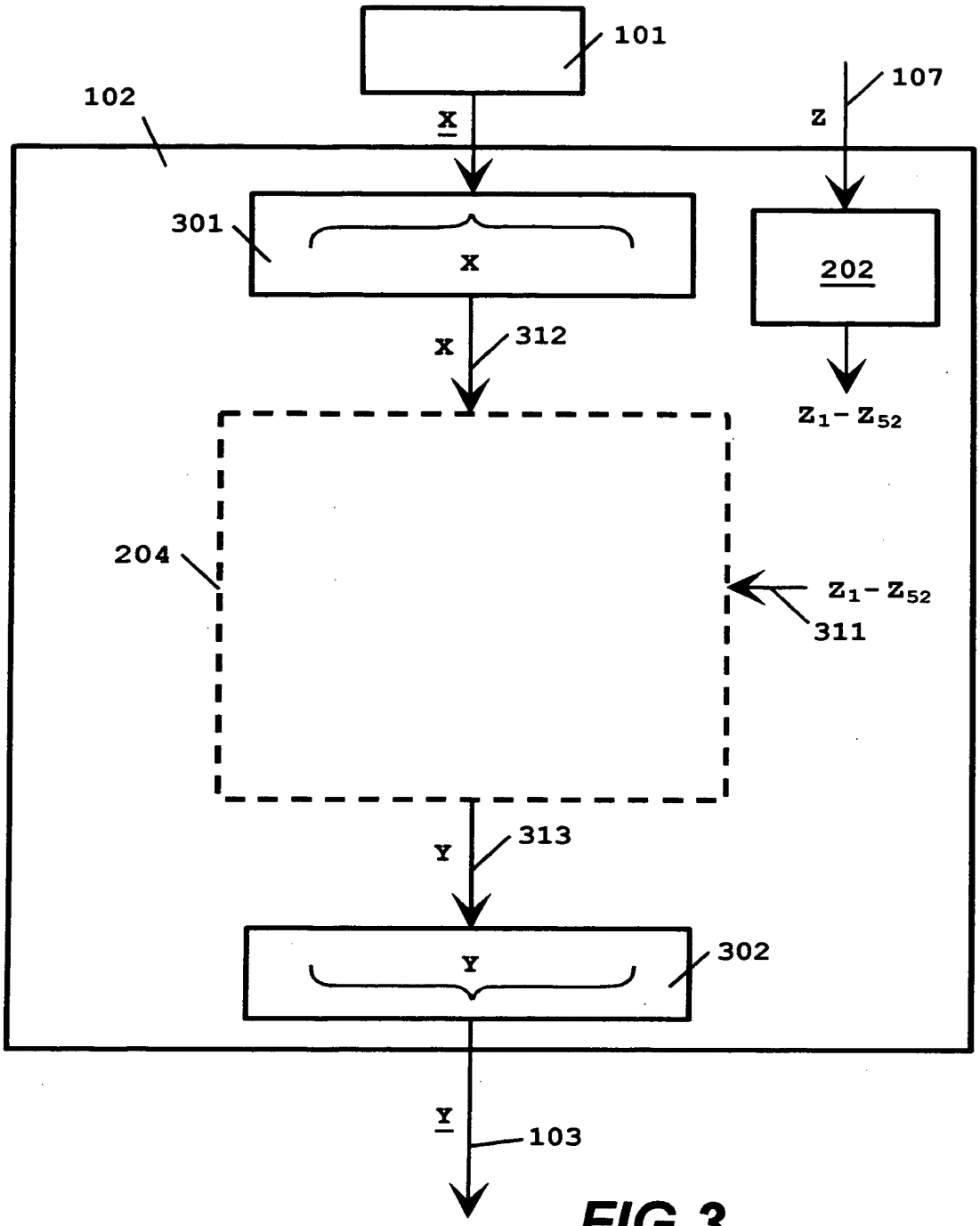

FIG.3
ARTE PREVIO

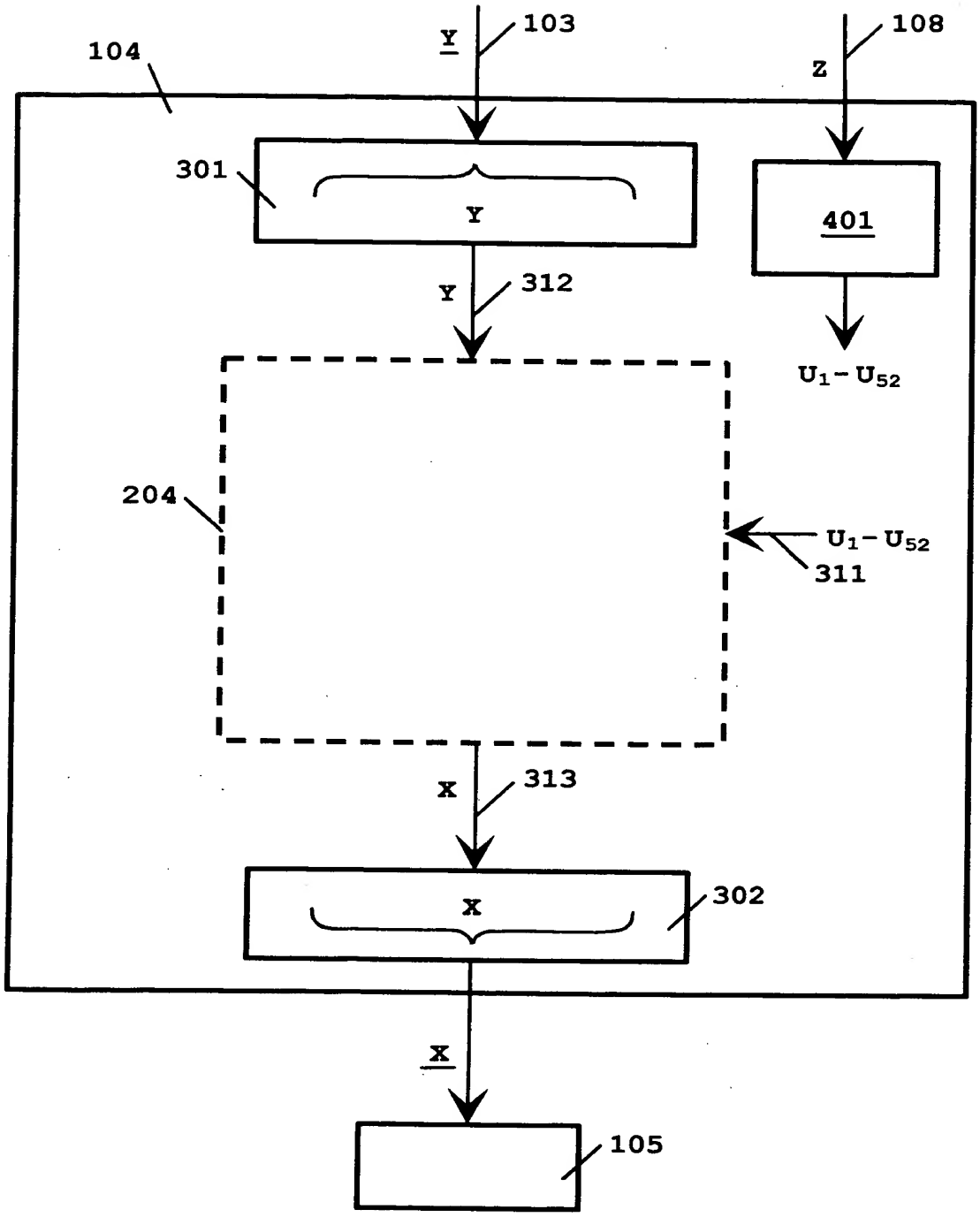

FIG.4
ARTE PREVIO

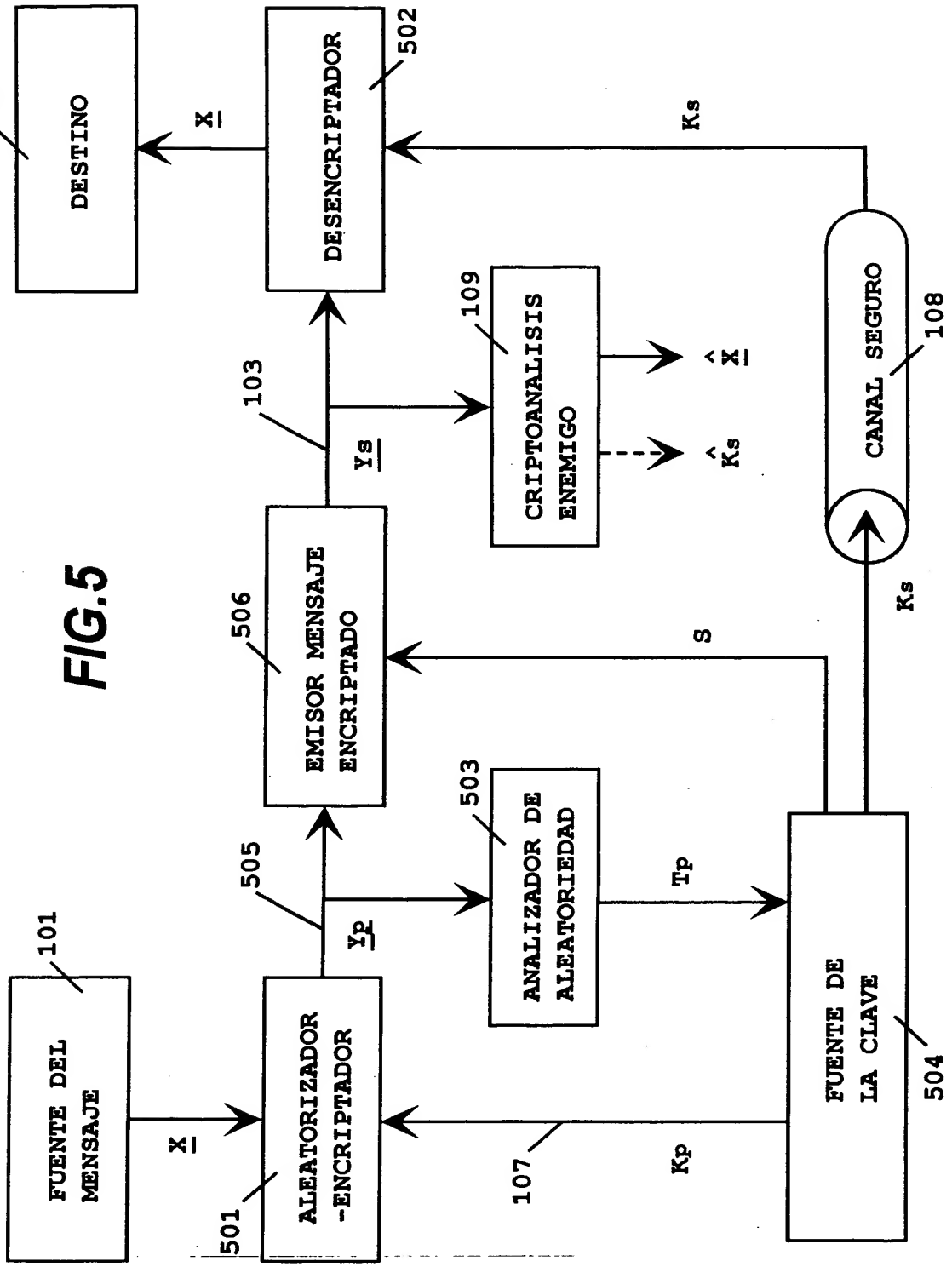
FUENTE DEL MENSAJE
101
ALEATORIZADOR -ENCRIPTADOR
501
EMISOR MENSAJE ENCRIPTADO
506
DESENCRIPTADOR
502
DESTINO
105
ANALIZADOR DE ALEATORIEDAD
503
CRIPTOANALISIS ENEMIGO
109
FUENTE DE LA CLAVE
504
CANAL SEGURO
108
X
Yp
Ys
Tp
S
Ks
Kp
107
505
103

FIG.5

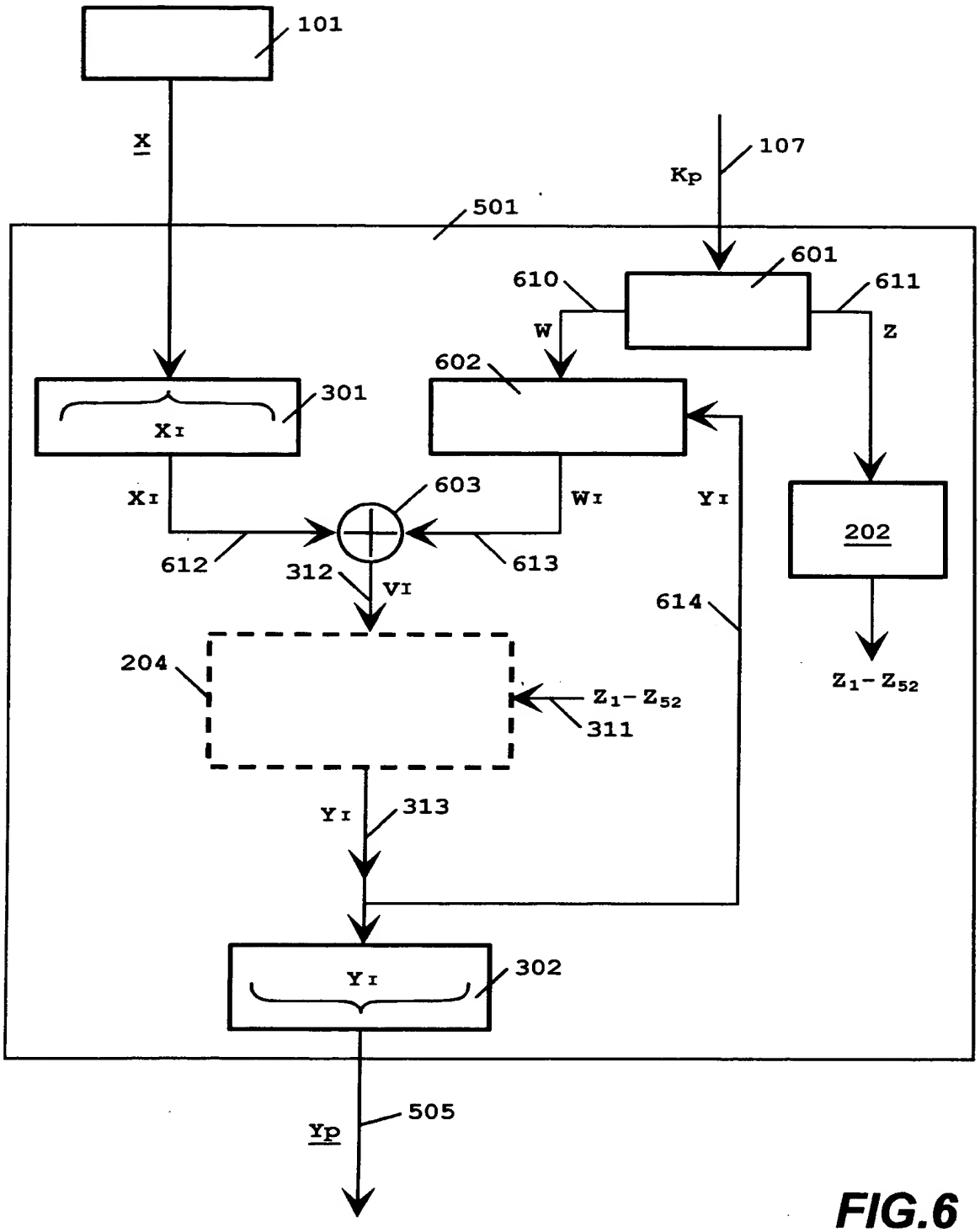
101
X
107
Kp
501
601
610
611
W
Z
602
301
XI
603
XI
WI
YI
202
612
312
613
VI
614
204
Z1 - Z52
311
Z1 - Z52
YI
313
YI
302
505
Yp

FIG.6

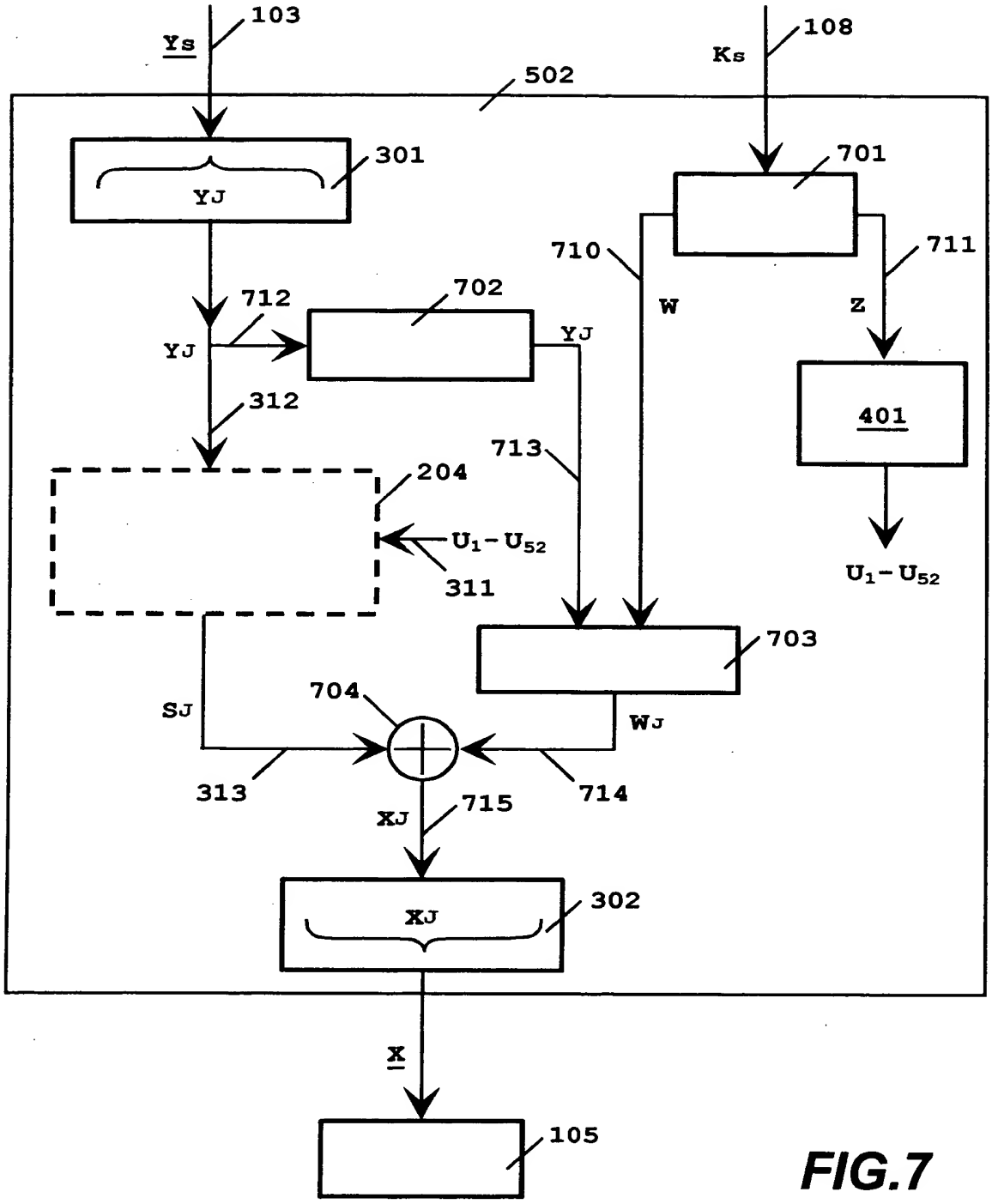
Ys
103
Ks
108
502
301
YJ
701
710
711
W
Z
712
YJ
702
YJ
312
401
713
204
U1 - U52
311
U1 - U52
703
SJ
704
WJ
313
714
715
XJ
302
XJ
X
105

FIG.7

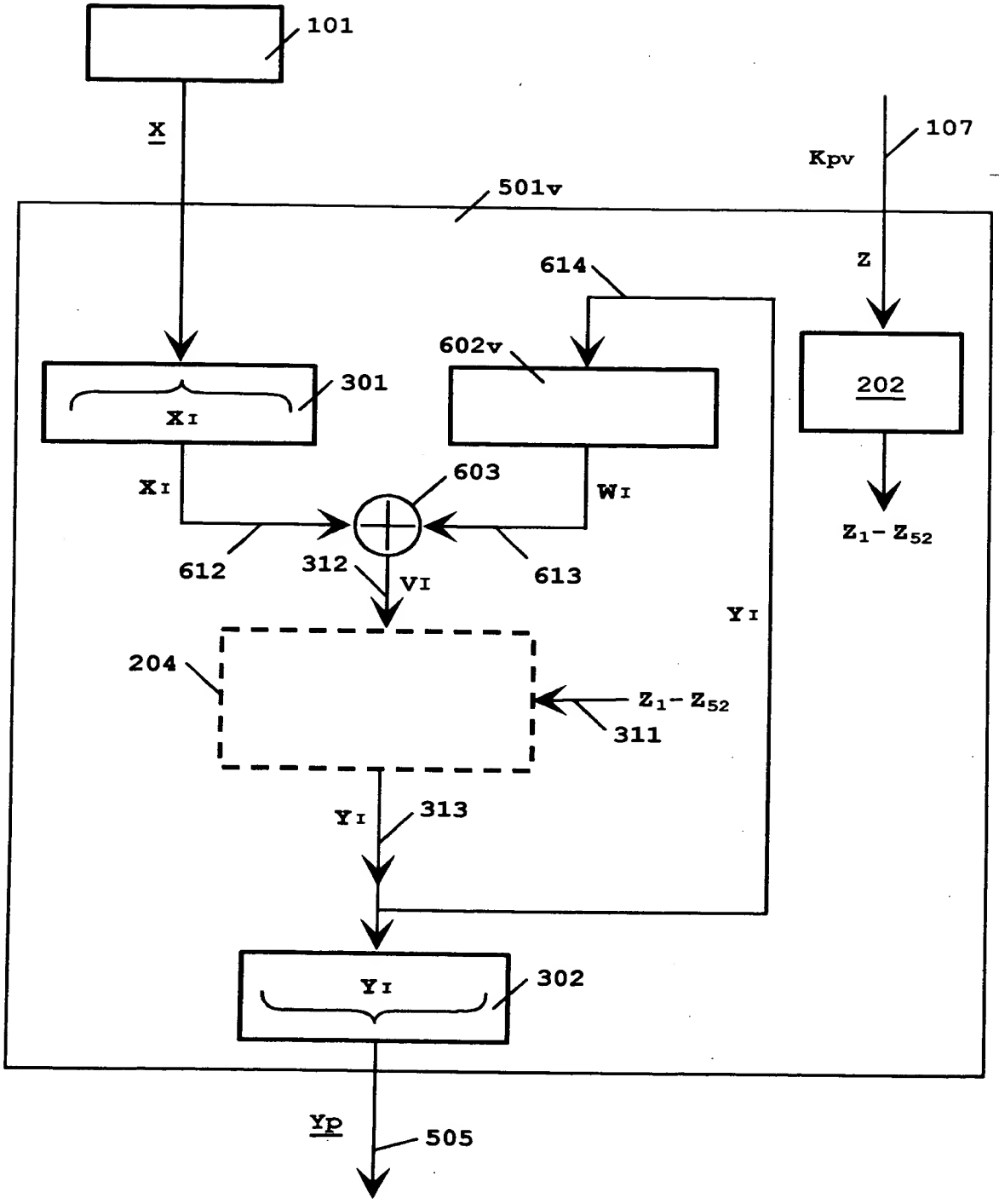
101
X
Kpv
107
501v
614
Z
602v
301
202
XI
603
WI
XI
Z1 - Z52
612
312
613
VI
YI
204
Z1 - Z52
311
YI
313
YI
302
Yp
505

FIG.8

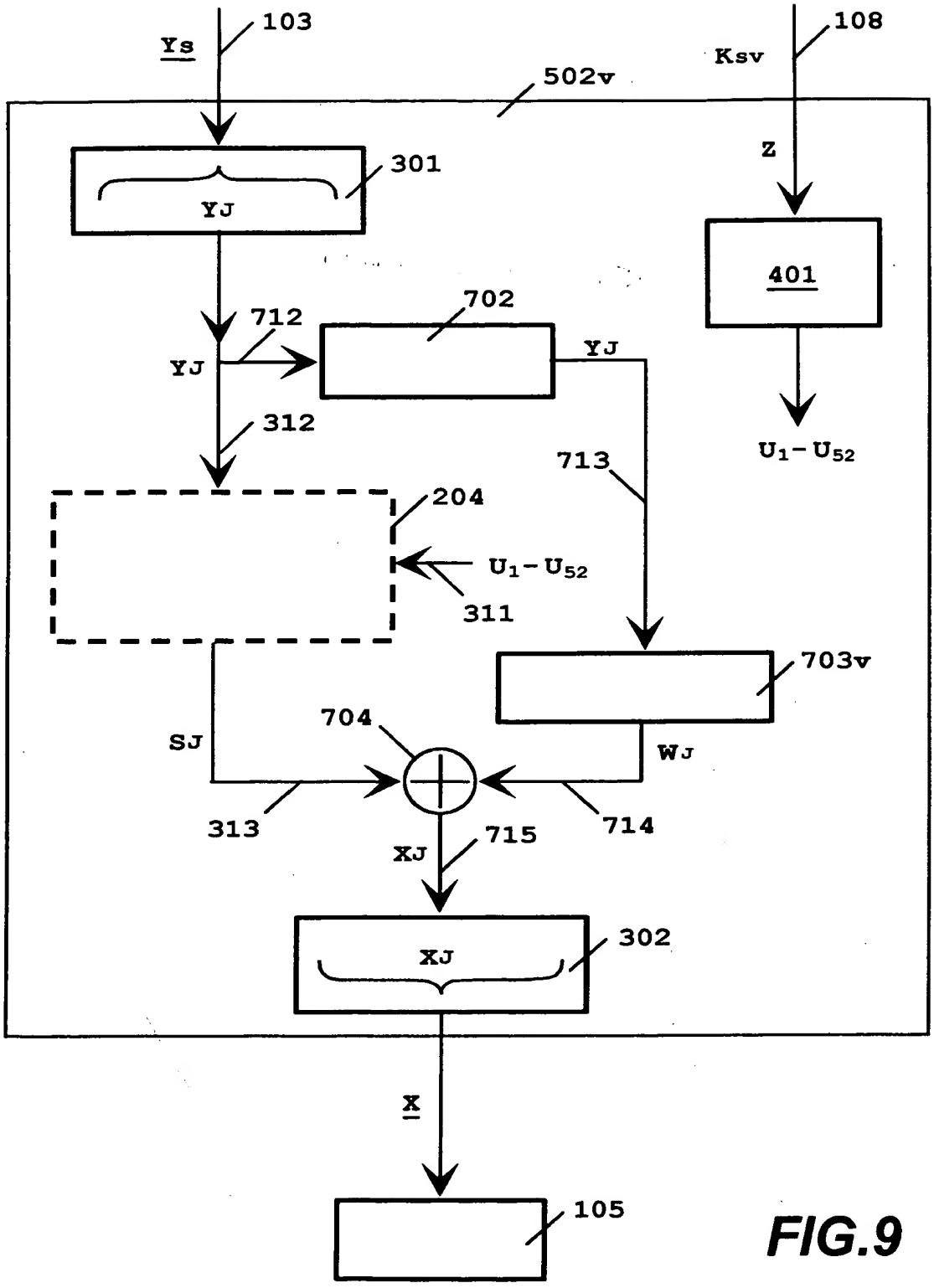
Ys
103
Ksv
108
502v
301
YJ
Z
401
712
702
YJ
YJ
312
U1 – U52
713
204
U1 – U52
311
703v
704
SJ
WJ
313
714
715
XJ
302
XJ
X
105

FIG.9